aws

Guide de l’utilisateur

Amazon Simple Storage Service



Version de l'API 2006-03-01

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon Simple Storage Service: Guide de l’utilisateur

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d’Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n’est pas d’Amazon, d’une manière susceptible de créer une confusion parmi 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 qu'Amazon S3 ? 1
Fonctions d'Amazon S3 1
Classes de stockage 1
Gestion du stockage 2
Gestion des accès et sécurité 3
Traitement des données 4
Journalisation et surveillance du stockage 4
Analytique et informations 5
Forte cohérence 6
Fonctionnement d'Amazon S3 6
Compartiments 7
Objets 10
Clés 10
Gestion des versions S3 11
ID de version 11
Politique de compartiment 11
Points d'accès S3 12
Listes de contrôle d'accès (ACLs) 12
Régions 13
Modèle de cohérence des données Amazon S3 13
Applications simultanées 15
Services connexes 16
Accès à Amazon S3 17
AWS Management Console 17
AWS Command Line Interface 17
AWS SDKs 18
API REST Amazon S3 18
Paiement pour Amazon S3 19
Conformité PCI DSS 19
Premiers pas 21
Configuration 21
Inscrivez-vous pour un Compte AWS 22
Création d'un utilisateur doté d'un accès administratif 22
Étape 1 : créer un compartiment 24

Étape 2 : charger un objet 31
Étape 3 : télécharger un objet 32
Utilisation de la console S3 33
Étape 4 : copier un objet 34
Étape 5 : supprimer les objets et le compartiment 35
Suppression d'un objet 36
Vider votre compartiment 36
Suppression de votre compartiment 37
Étapes suivantes 37
Comprendre les cas d'utilisation courants 38
Contrôlez l'accès à vos compartiments et à vos objets 38
Protection et surveillance de votre stockage 39
Développer avec Amazon S3 40
Apprendre à partir de tutoriels 41
Explorer la formation et le support 43
Utilisation d'Amazon S3 avec le AWS CLI 43
Configuration 44
Étape 1 : créer votre premier compartiment Amazon S3 45
Étape 2 : charger un objet dans votre compartiment 51
Étape 3 : télécharger un objet 52
Étape 4 : copier votre objet dans un dossier 53
Étape 5 : supprimer vos objets et votre compartiment 54
Étapes suivantes 57
Utilisation de seaux à usage général 59
Présentation des compartiments à usage général 60
Présentation des compartiments à usage général 61
Modèles de seaux à usage général courants 62
Autorisations 62
Gestion de l'accès du public aux compartiments à usage général 63
Configuration des godets à usage général 64
Fonctionnement des godets à usage général 68
Surveillance des performances des godets à usage général 68
Modèles de compartiments courants 69
Modèle de compartiment à usage général pour plusieurs locataires 70
Bucket-per-use motif 71
Règles de dénomination 72

Règles de dénomination des compartiments à usage général 72
Exemples de noms de compartiments à usage général 74
Bonnes pratiques 75
Création d'un compartiment qui utilise un GUID dans son nom 77
Quotas, restrictions et limitations 78
Quotas de compartiments 78
Limitations sur les objets et compartiments 79
Règles d'attribution de noms pour les compartiments 79
Accès aux compartiments 79
..... 79
Hébergement virtuel de buckets à usage général 83
Création d'un bucket à usage général 93
Réglages du godet à usage général 93
Affichage des propriétés d'un compartiment 108
Affichage des compartiments 111
Vidange d'un seau à usage général 118
Vidange d'un godet à usage général avec une configuration AWS CloudTrail 121
Supprimer un bucket à usage général 121
Mountpoint pour Amazon S3 128
Installation de Mountpoint 129
Configuration et utilisation de Mountpoint 134
Dépannage de Mountpoint 140
Navigateur de stockage pour Amazon S3 141
Utilisation du navigateur de stockage pour S3 142
Installation du navigateur de stockage pour S3 143
Configuration du navigateur de stockage pour S3 144
Configuration du navigateur de stockage pour S3 159
Résolution des problèmes liés au navigateur de stockage pour S3 160
Configuration de l'accélération des transferts 160
Pourquoi utiliser Transfer Acceleration ? 161
Conditions d'utilisation de Transfer Acceleration 161
Premiers pas 163
Activation de Transfer Acceleration 165
Outil de comparaison de vitesse 173
Utiliser le paiement du demandeur 173
Fonctionnement du Paiement par le demandeur 175

Configuration de Paiement par le demandeur 175
Récupérer la configuration requestPayment 177
Téléchargement d'objets à partir de compartiments de type Paiement par le demandeur 178
Utilisation des objets 181
Présentation des objets 182
Sous-ressources 183
Attribution d'un nom aux objets 184
Choix des noms de clés d'objet 185
Directives de dénomination de la clé d'objet 186
Utilisation des métadonnées 189
Métadonnées d'objet définies par le système 191
Métadonnées d'objet définies par l'utilisateur 194
Modification des métadonnées d'un objet 196
Accélération de la découverte des données 200
Chargement d'objets 297
Charger un objet 298
Empêcher le chargement d'objets portant des noms de clé identiques 311
Utilisation du chargement partitionné 312
Demandes conditionnelles 392
Comment récupérer ou copier des objets en fonction des métadonnées 393
Comment empêcher le remplacement d'objets 395
Copie, déplacement et changement de nom des objets 406
Pour copier un objet 409
Pour déplacer un objet 420
Pour renommer un objet 422
Téléchargement d'objets 423
Téléchargement d'un objet 424
Téléchargement de plusieurs objets 426
Téléchargement d'une partie d'un objet 428
Téléchargement d'un objet à partir d'un autre Compte AWS 429
Téléchargement des objets archivés 430
Téléchargement d'objets en fonction des métadonnées 430
Résolution des problèmes de téléchargement d'objets 431
Vérification de l'intégrité des objets dans Amazon S3 431
Utilisation des algorithmes de total de contrôle pris en charge 432
Types de sommes de contrôle d'objet entier et composites 433

Utilisation des sommes de contrôle des objets entiers pour le chargement partitionné 436
Utilisation des sommes de contrôle au niveau des parties d'un chargement partitionné 437
Opérations de somme de contrôle 438
Utilisation de Content- MD5 lors du téléchargement d'objets 446
Utilisation du contenu MD5 et du ETag pour vérifier les objets téléchargés 447
Utilisation des totaux de contrôle de fin 447
Suppression d'objets 454
Bonnes pratiques à prendre en compte avant de supprimer un objet 454
Suppression d'objets à partir d'un compartiment avec gestion des versions activée 456
Suppression d'objets à partir d'um compartiment avec gestion des versions désactivée 456
Suppression d'objets à partir d'un compartiment sans gestion des versions 456
Suppression des objets d'un compartiment avec authentification MFA activée 457
Suppression d'un seul objet 457
Suppression de plusieurs objets 470
Organisation et liste des objets 473
Utilisation de préfixes 473
Liste des objets 476
Utilisation de dossiers 479
Affichage des propriétés d'un objet 484
Catégorisation des objets à l'aide de balises 486
Utilisation du présigné URLs pour télécharger et charger des objets 501
Utilisateurs habilités à créer une URL présignée 502
Date d'expiration du présigné URLs 503
Limitation des capacités des URL présignées 503
Partage d'objets avec présigné URLs 505
Téléchargement d'objets présignés URLs 510
Transformation d'objets 514
Création de points d'accès Object Lambda 516
Utilisation des points d'accès Amazon S3 Object Lambda 531
Considérations sur la sécurité 535
Écriture de fonctions Lambda 543
Utilisation des fonctions AWS intégrées 575
Bonnes pratiques et directives pour S3 Object Lambda 577
Didacticiels S3 Object Lambda 579
Débogage de S3 Object Lambda 618
Exécution d'opérations groupées sur des objets 619

Principes de base des opérations par lot 620
Tutoriel des opérations par lots S3 622
Octroi d'autorisations 622
Création d'une tâche 633
Opérations prises en charge 657
Gestion des tâches 704
Suivi de l'état de la tâche et des rapports de fin de tâche 709
Utilisation d'étiquettes 725
Gestion du verrouillage d'objet à l'aide des opérations par lot 742
Didacticiel : transcodage par lot de vidéos 767
Résolution des problèmes d'opérations par lot 810
Interrogation des données sur place 813
Exigences et limites 814
Création d'une demande 815
Erreurs 816
Exemples S3 Select 816
Référence SQL 821
Utilisation des compartiments de répertoires 863
Noms des compartiments de répertoires 864
Annuaires 864
Noms de clés 865
Gestion des accès 865
Quotas de compartiments de répertoires 865
Création et utilisation de compartiments de répertoires 866
Cas d'utilisation des compartiments de répertoires 867
Charges de travail hautes performances 868
Charges de travail liées à la résidence des données 928
Différences pour les compartiments de répertoires 946
Différences pour les compartiments de répertoires 947
Opérations d'API prises en charge pour les compartiments de répertoires 949
Fonctionnalités Amazon S3 non prises en charge par les compartiments de répertoires 949
Mise en réseau des compartiments de répertoires 950
Points de terminaison 951
Configuration de points de terminaison de VPC de passerelle 951
Règles de dénomination des compartiments de répertoires 952
Affichage des propriétés 953

Gestion des politiques de compartiment 954
Ajout d'une politique de compartiment 954
Affichage d'une politique de compartiment 958
Suppression d'une politique de compartiment 958
Vidage d'un compartiment de répertoires 959
Suppression d'un compartiment de répertoires 960
Établissement de la liste des compartiments de répertoires 963
Déterminer si vous pouvez accéder à un compartiment 966
Utilisation d'objets dans un compartiment de répertoires 967
Importation d'objets dans un compartiment de répertoires 968
Utilisation du cycle de vie S3 970
Utilisation des opérations par lots avec S3 Express One Zone 983
Ajout de données à des objets 987
Modification du nom d'un objet 989
Chargement d'un objet 996
Copier un objet 1030
Suppression d'un objet 1036
Téléchargement d'un objet 1040
Génération d'objets présignés URLs pour partager 1043
Récupération des métadonnées d'un objet 1043
Liste des objets 1044
Sécurité des compartiments de répertoires 1045
Protection et chiffrement des données 1045
Authentification et autorisation des demandes 1071
Bonnes pratiques de sécurité 1083
Utilisation de points d'accès pour les compartiments de répertoires 1087
Règles, restrictions et limitations de dénomination 1088
Référencement des points d'accès pour les compartiments de répertoire 1090
Opérations sur les objets des points d'accès 1091
Configuration des politiques IAM 1091
Surveillance et journalisation 1098
Création de points d'accès pour les compartiments de répertoires 1099
Gestion des points d'accès 1104
Marquage des points d'accès 1119
Journalisation avec AWS CloudTrail des compartiments de répertoire 1135
CloudTrail événements de gestion pour les compartiments de répertoire 1136

CloudTrail événements de données pour les compartiments de répertoire 1137
..... 1138
Optimisation des performances des compartiments de répertoires 1145
Utilisation de l'authentification basée sur les sessions 1145
Bonnes pratiques supplémentaires en matière de somme de contrôle S3 1146
Utiliser la dernière version des bibliothèques d'exécution AWS SDKs et les bibliothèques d'exécution communes 1146
Développement avec des compartiments de répertoires 1146
Points de terminaison d'API régionaux et zonaux des compartiments de répertoires 1147
Utilisation de compartiments de répertoires à l'aide de la console S3 AWS CLI, et AWS SDKs 1148
Opérations d'API des compartiments de répertoires 1150
Balisage des buckets de répertoires 1152
Méthodes courantes d'utilisation des balises avec les compartiments de répertoire 1152
Gestion des balises pour les compartiments de répertoires 1156
Création de compartiments de répertoire avec des balises 1157
Ajouter une balise à un bucket de répertoire 1161
Affichage des balises de bucket du répertoire 1164
Supprimer un tag d'un bucket de répertoire 1167
Utilisation d'Amazon S3 Tables et des compartiments de tables 1171
Fonctionnalités de S3 Tables 1172
Services connexes 1173
Didacticiel : Premiers pas avec S3 Tables 1174
Étape 1 : créer un bucket de tables et l'intégrer aux services AWS d'analyse 1175
Étape 2 : Création d'un espace de noms de table et d'une table 1176
(Facultatif) Étape 3 : Accordez les autorisations de Lake Formation sur votre table 1179
Étape 4 : Interroger des données avec SQL dans Athena 1181
Compartiments de tables 1182
Types de seaux de table 1183
Règles de dénomination des compartiments de tables 1184
Créer un compartiment de tables 1186
Supprimer un compartiment de tables 1189
Affichage des détails d'un compartiment de tables 1189
Gestion des politiques 1190
AWS seaux de table gérés 1191
Maintenance de S3 Tables 1195

Statut des tâches de maintenance de S3 Tables ... 1196
Maintenance des compartiments de tables ... 1197
Maintenance des tables ... 1199
Considérations et restrictions ... 1205
Espaces de noms ... 1207
Création d'un espace de noms ... 1208
Suppression d'un espace de noms ... 1210
Tables ... 1211
Créer une table ... 1212
Supprimer une table ... 1218
Gestion des politiques ... 1219
Accès aux tables ... 1221
Accès aux tables via l'intégration Amazon SageMaker Lakehouse ... 1221
Accès direct aux tables ... 1223
Utilisation de tables S3 avec des services AWS d'analyse ... 1224
Accès aux tables à l'aide du AWS GlueIceberg REST point de terminaison ... 1238
Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison ... 1243
Accès aux tables avec le catalogue client ... 1250
Amazon Athena ... 1252
Amazon Redshift ... 1254
Amazon EMR ... 1255
QuickSight ... 1259
Amazon Data Firehose ... 1262
AWS Glue ETL ... 1268
points de terminaison,Régions AWS et quotas ... 1279
Tables Régions AWS et points de terminaison S3 ... 1279
Quotas des tables S3 ... 1284
Sécurité pour S3 Tables ... 1285
Chiffrement ... 1287
Gestion des accès ... 1302
Connectivité VPC ... 1333
Restrictions et limitations ... 1337
Journalisation avec AWS CloudTrail pour les tables S3 ... 1338
CloudTrail événements de gestion pour les tables S3 ... 1338
CloudTrail événements de données pour les tables S3 ... 1340
CloudTrail exemples de journaux ... 1341

Utilisation de vecteurs S3 et de buckets vectoriels 1345
Qu'est-ce qu'Amazon S3 Vectors ? 1345
Cas d'utilisation : recherches de similarité dans de grands ensembles de données 1346
Caractéristiques des vecteurs S3 1347
Stockage spécialement conçu pour les vecteurs 1347
Réaliser des requêtes de similarité 1347
Filtrage des métadonnées 1347
Gestion des accès et sécurité 1348
Intégration aux AWS services 1348
Tutoriel : Débuter avec les vecteurs S3 1348
Étape 1 : créer un bucket vectoriel avec la console 1349
Étape 2 : créer un index vectoriel dans un bucket vectoriel avec la console 1350
Étape 3 : Insérer des vecteurs dans un index vectoriel avec le SDK pour Python (SDK for Python) 1352
Étape 4 : Vecteurs de requête dans un index vectoriel avec le SDK pour Python (Boto3) .. 1354
(Facultatif) Automatisez la création d'intégrations vectorielles avec la CLI S3 Vectors Embed 1356
(Facultatif) Intégrez les vecteurs S3 aux bases de connaissances Amazon Bedrock 1356
(Facultatif) Intégrez les vecteurs S3 à Amazon OpenSearch 1359
Seaux vectoriels 1359
Règles de dénomination des compartiments vectoriels 1361
Création d'un bucket vectoriel 1362
Répertorier les seaux vectoriels 1365
Affichage des attributs d'un bucket vectoriel 1366
Supprimer un bucket vectoriel 1366
Gestion des politiques relatives aux compartiments vectoriels 1367
Indices vectoriels 1369
Exigences relatives à la dénomination des index vectoriels 1370
Exigences relatives aux dimensions 1370
Options de mesure de distance 1370
Clés de métadonnées non filtrables 1370
Création d'un index vectoriel dans un compartiment vectoriel 1372
Répertorier les index vectoriels 1376
Supprimer un index vectoriel 1379
Vecteurs 1380
Concepts vectoriels 1380

Insertion de vecteurs dans un index vectoriel ... 1381
Vecteurs de listes ... 1384
Vecteurs d'interrogation ... 1386
Supprimer des vecteurs d'un index vectoriel ... 1389
Filtrage des métadonnées ... 1390
Limites et restrictions ... 1394
Meilleures pratiques en matière de vecteurs S3 ... 1396
Création et recherche d'intégrations vectorielles avec `s3vectors-embed-cli` ... 1397
Utilisation de vecteurs S3 avec d'autres AWS services ... 1398
Intégrations disponibles ... 1398
Avantages de l'intégration ... 1399
Utilisation de vecteurs S3 avec OpenSearch Service ... 1399
Utilisation de vecteurs S3 avec les bases de connaissances Amazon Bedrock ... 1403
Régions AWS, points de terminaison et quotas pour les vecteurs S3 ... 1408
AWS Régions et points de terminaison S3 Vectors ... 1408
Quotas de service S3 Vectors ... 1410
La sécurité dans les vecteurs S3 ... 1410
Gestion des identités et des accès dans S3 Vectors ... 1411
Protection des données et chiffrement dans S3 Vectors ... 1429
Journalisation avec AWS CloudTrail for S3 Vectors ... 1437
Informations sur les vecteurs S3 dans CloudTrail ... 1437
CloudTrail événements de gestion pour S3 Vectors ... 1438
CloudTrail événements de données pour les vecteurs S3 ... 1439
Activation de la journalisation des événements de données pour les vecteurs S3 ... 1440
CloudTrail exemple de fichier journal pour les vecteurs S3 ... 1441
Contrôle d'accès ... 1444
Ressources S3 ... 1445
Identités ... 1450
Propriétaires du compartiment ou de la ressource ... 1452
Outils de gestion des accès ... 1453
Actions ... 1460
Cas d'utilisation de la gestion des accès ... 1461
Résolution des problèmes de gestion d'accès ... 1468
Identity and Access Management (IAM) ... 1470
Public ciblé ... 1471
Authentification par des identités ... 1472

Gestion des accès à l'aide de politiques ... 1476
Fonctionnement d'Amazon S3 avec IAM ... 1479
Demande d'autorisation ... 1509
Autorisations requises pour les opérations d'API S3 ... 1519
Politiques et autorisations ... 1566
Politiques de compartiment ... 1571
Politiques basées sur l'identité ... 1624
Procédures détaillées qui utilisent des politiques ... 1664
Utilisation des rôles liés à un service pour Amazon S3 Storage Lens ... 1709
Résolution des problèmes d'identité et d'accès Amazon S3 ... 1713
AWS politiques gérées ... 1740
Utilisation des points d'accès ... 1743
Règles, restrictions et limitations de dénomination ... 1744
Référencement des points d'accès ... 1748
Compatibilité avec les points d'accès ... 1752
Configuration des stratégies IAM ... 1754
Surveillance et journalisation ... 1763
Création d'un point d'accès ... 1765
Gestion des points d'accès ... 1773
Utilisation des points d'accès ... 1779
Marquage des points d'accès ... 1792
Gestion de l'accès avec les autorisations d'accès S3 ... 1809
Concepts des autorisations d'accès S3 ... 1811
Autorisations d'accès S3 et identités d'annuaire d'entreprise ... 1816
Bien démarrer avec les autorisations d'accès S3 ... 1825
Utilisation des instances d'autorisations d'accès S3 ... 1827
Utilisation des emplacements d'autorisations d'accès S3 ... 1840
Octroi d'autorisations avec les autorisations d'accès S3 ... 1864
Obtention de données S3 à l'aide d'autorisations d'accès ... 1878
Accès intercompte aux autorisations d'accès S3 ... 1895
Gestion des balises pour les subventions d'accès S3 ... 1908
Limitations des autorisations d'accès S3 ... 1911
Intégrations des autorisations d'accès S3 ... 1913
Gérer l'accès avec ACLs ... 1915
Présentation des ACL ... 1916
Configuration ACLs ... 1939

Exemples de politiques 1958
Blocage de l'accès public 1963
Paramètres de la fonctionnalité de blocage de l'accès public 1965
Exécution d'opérations de blocage d'accès public sur un point d'accès 1969
La signification du mot « public » 1970
Utilisation de l'analyseur d'accès IAM pour S3 pour passer en revue les compartiments publics 1973
Autorisations 1974
Configuration du blocage d'accès public 1975
Configuration des paramètres de compte 1975
Configuration des paramètres de compartiment et de point d'accès 1978
Examen de l'accès au compartiment 1982
Révision de l'accès externe à l'aide d'un résumé des accès externes 1984
Informations fournies par IAM Access Analyzer pour S3 1986
Blocage de tous les accès publics 1987
Vérification et modification de l'accès à un compartiment 1988
Archivage des résultats de compartiment 1990
Activation d'un résultat de compartiment archivé 1990
Affichage des détails de résultats 1991
Téléchargement d'un rapport de l'analyseur d'accès IAM pour S3 1991
Vérification de la propriété du compartiment 1992
Quand utiliser la condition propriétaire du compartiment 1992
Vérification d'un propriétaire du compartiment 1993
Exemples 1994
Limites et restrictions 1997
Contrôle de la propriété des objets 1997
Paramètres de la propriété de l'objet 1999
Modifications apportées par la désactivation ACLs 2002
Conditions préalables à la désactivation ACLs 2004
Autorisations de propriété d'objet 2005
Désactivation ACLs pour tous les nouveaux buckets 2005
Réplication et propriété d'objet 2005
Définition de la propriété de l'objet 2006
Conditions préalables à la désactivation ACLs 2007
Créer un compartiment 2023
Définition de la propriété de l'objet 2033

Affichage des paramètres de la propriété de l'objet ... 2037
Désactivation ACLs pour tous les nouveaux buckets ... 2039
Résolution des problèmes ... 2042
Sécurité ... 2045
Bonnes pratiques de sécurité ... 2047
Bonnes pratiques en matière de sécurité Amazon S3 ... 2047
Bonnes pratiques de surveillance et d'audit pour Amazon S3 ... 2054
Surveillance de la sécurité des données ... 2058
Protection des données ... 2061
Chiffrement des données ... 2063
Chiffrement côté serveur ... 2065
Utilisation du chiffrement côté client ... 2171
Confidentialité du trafic inter-réseau ... 2172
Trafic entre les clients de service et sur site et les applications ... 2172
Trafic entre les AWS ressources d'une même région ... 2172
AWS PrivateLink pour Amazon S3 ... 2173
Validation de conformité ... 2192
Résilience ... 2194
Chiffrement des sauvegardes ... 2196
Sécurité de l'infrastructure ... 2197
Configuration et analyse des vulnérabilités ... 2198
Gestion des accès ... 2198
Protection des données ... 2202
Réplication d'objets au sein des régions et entre elles ... 2204
Pourquoi utiliser la réplication ? ... 2205
Quand utiliser la réplication entre Régions ... 2207
Quand utiliser la réplication au sein d'une même Région ... 2207
Quand utiliser la réplication à double sens (réplication bi-directionnelle) ... 2208
Quand utiliser la réplication par lot S3 ... 2209
Exigences relatives à la charge de travail et réplication en direct ... 2209
Ce qui est répliqué ... 2210
Exigences et considérations relatives à la réplication ... 2214
Configuration de la réplication en direct ... 2218
Gestion ou suspension de la réplication en direct ... 2318
Réplication d'objets existants ... 2320
Résolution des problèmes de réplication ... 2336

Surveillance de la progression et obtention du statut 2345
Gestion du trafic multirégional 2372
Création de points d'accès multi-Régions 2374
Configuration de points d'accès multi-régions 2385
Utilisation de points d'accès multi-régions 2392
Conservation de plusieurs versions d'objets 2449
Compartiments non versionnés, activés pour la gestion des versions et suspendus 2450
Utilisation de la gestion des versions S3 avec le cycle de vie S3 2451
Gestion des versions S3 2452
Activation de la gestion des versions sur les compartiments 2456
Configuration de la fonction Supprimer MFA 2464
Utilisation des objets compatibles avec la gestion des versions 2467
Utilisation d'objets dont la gestion des versions est désactivée 2498
Résolution des problèmes de gestion des versions 2503
Verrouillage d'objets 2508
Fonctionnement du verrouillage d'objets S3 2509
Considérations relatives au verrouillage d'objet 2514
Configuration du verrouillage des objets 2520
Sauvegarde des données 2532
Optimisation des coûts 2534
Rapports d'utilisation et de facturation 2535
Utilisation des balises de répartition des coûts 2536
Rapports de facturation 2538
Rapports d'utilisation 2542
Présentation des rapports d'utilisation et de facturation 2544
Facturation des réponses d'erreur Amazon S3 2572
Bien comprendre et gérer les classes de stockage 2597
Objets fréquemment consultés 2597
Optimisation automatique des données avec des modèles d'accès inconnus ou irréguliers 2598
Objets rarement consultés 2600
Objets rarement consultés 2602
Amazon S3 sur Outposts 2603
Comparaison des classes de stockage 2604
Définition de la classe de stockage d'un objet 2605
Analyse de classe de stockage 2610
Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering 2618

Classes de stockage Amazon S3 Glacier 2631
Utilisation des objets archivés 2638
Gestion du cycle de vie 2652
Gestion du cycle de vie complet des objets 2654
Transition des objets 2655
Objets en cours d'expiration 2664
Définition d'une configuration de cycle de vie 2667
Utilisation d'autres configurations de compartiment 2687
Configuration des notifications d'événements du cycle de vie S3 2690
Éléments de la configuration du cycle de vie 2692
Conflits de configurations du cycle de vie 2711
Exemples de configurations du cycle de vie S3 2716
Résolution des problèmes du cycle de vie 2733
Journalisation et surveillance 2741
Outils de surveillance 2745
Outils automatisés 2745
Outils manuels 2746
Options de journalisation 2747
Se connecter avec CloudTrail 2750
Utilisation de CloudTrail journaux avec les journaux d'accès au serveur Amazon S3 et CloudWatch les journaux 2752
CloudTrail suivi avec les appels d'API SOAP Amazon S3 2753
CloudTrail événements 2754
Exemples de fichiers journaux 2767
Activant CloudTrail 2771
Identification des demandes S3 2775
Enregistrement de l'accès au serveur 2783
Comment activer la livraison des journaux ? 2784
Format de clé d'objet journal 2787
Comment sont distribués les journaux ? 2787
Livraison des journaux du serveur dans la mesure du possible 2788
Les changements de statut de la journalisation des compartiments prennent effet au fil du temps 2789
Activation de la journalisation des accès au serveur 2790
Format des journaux 2814
Suppression des fichiers journaux 2829

Identification des demandes S3 2830
Résolution des problèmes de journalisation des accès au serveur 2838
Surveillance des métriques avec CloudWatch 2841
Métriques et dimensions 2844
Accès aux CloudWatch métriques 2864
CloudWatch configurations de métriques 2865
Notifications d'événements Amazon S3 2875
Présentation 2876
Types de notification et destinations associées 2877
Utilisation de SQS, SNS et Lambda 2885
En utilisant EventBridge 2917
Visualisation de l'activité et de l'utilisation du stockage 2928
Métriques et fonctionnalités S3 Storage Lens 2929
Présentation de S3 Storage Lens 2931
Glossaire des métriques 2944
Définition des autorisations d' 2981
Utilisation de S3 Storage Lens 2986
Afficher les métriques de stockage 3027
Utilisation d'Organizations 3091
Utilisation des groupes Storage Lens 3102
Catalogage et analyse de vos données 3148
Compartiments d'inventaire Amazon S3 3149
Listes d'inventaire 3150
Configuration de l'inventaire Amazon S3 3156
Localisation de votre inventaire 3167
Configuration des notifications pour la publication d'un inventaire 3171
Interrogation d'un inventaire avec Athena 3172
Conversion de chaînes d'ID de version vides en chaînes null 3178
Utiliser le champ Liste ACL d'objet 3181
Optimisation des performances 3184
Recommandations de performance pour Amazon S3 3185
Mesurer les performances 3186
Mise à l'échelle horizontale 3187
Utilisation des extractions de plages d'octets 3187
Nouvelle tentative de demandes 3187
Combinez Amazon S3 et Amazon EC2 dans la même région 3188

Utilisation de Transfer Acceleration pour réduire la latence 3188
Utilisez la dernière version AWS SDKs 3188
Modèles de conception des performances pour Amazon S3 3189
Mise en cache du contenu consulté fréquemment 3189
Délais d'expiration et nouvelles tentatives pour les applications sensibles à la latence 3190
Mise à l'échelle horizontale et mise en parallèle des demandes 3191
Accélération des transferts de données disparates géographiquement 3193
Hébergement d'un site web statique 3195
Points de terminaison de sites web 3196
Exemples de point de terminaison de site web 3198
Ajout d'un DNS CNAME 3198
Utilisation d'un domaine personnalisé avec Route 53 3199
Différences clés entre un point de terminaison de site web et un point de terminaison de l'API REST 3199
Activation de l'hébergement de sites web 3200
Configuration d'un document d'index 3206
Document d'index et dossiers 3206
Configurer un document d'index 3207
Configuration d'un document d'erreur personnalisé 3209
Codes de réponse HTTP Amazon S3 3209
Configuration d'un document d'erreur personnalisé 3212
Définition des autorisations pour l'accès au site web 3213
Étape 1 : modifier les paramètres de blocage de l'accès public S3 3214
Étape 2 : ajouter une politique de compartiment 3216
Listes de contrôle d'accès à l'objet 3218
Journalisation du trafic Web 3219
Configuration d'une redirection 3220
Rediriger les demandes vers un autre hôte 3221
Configurer des règles de redirection 3222
Rediriger les demandes pour un objet 3230
Utilisation de CORS 3232
Partage des ressources de plusieurs origines : scénarios de cas d'utilisation 3233
Comment Amazon S3 évalue la configuration CORS sur un compartiment ? 3233
Comment le point d'accès Object Lambda prend en charge le CORS 3234
Éléments d'une configuration CORS 3234
Configuration de CORS 3240

Test du CORS 3249
Dépannage du CORS 3251
Didacticiels relatifs aux sites Web statiques 3257
Hébergement de vidéos en streaming 3258
Configuration d'un site web statique 3280
Configuration d'un site web statique à l'aide d'un domaine personnalisé 3289
Déploiement d'un site Web statique sur Amplify à partir d'Amazon S3 3317
Marquage des ressources S3 3320
Comment fonctionnent les tags 3320
Balises définies par l'utilisateur 3320
Méthodes courantes d'utilisation des balises 3322
Utilisation de balises pour la répartition des coûts 3323
Utilisation de balises pour le contrôle d'accès basé sur les attributs (ABAC) 3324
Planification de votre stratégie de marquage 3325
Gestion des balises pour les ressources Amazon S3 3326
Quotas 3328
Augmentations des quotas 3328
Référence 3329
Historique du document 3331
Mises à jour antérieures 3392
..... mmmcdxxiv

Qu'est-ce qu'Amazon S3 ?

Amazon Simple Storage Service (Amazon S3) est un service de stockage d'objets qui offre une capacité de mise à l'échelle, une disponibilité des données, une sécurité et des performances de pointe. Les clients de toutes tailles et secteurs peuvent utiliser Amazon S3 pour stocker et protéger toute quantité de données dans un large éventail de cas d'utilisation, par exemple des lacs de données, des sites Web, des applications mobiles, des sauvegardes et restaurations, des archives, des applications métier, des appareils IoT et l'analytique du big data. Amazon S3 offre des fonctions de gestion qui vous permettent d'optimiser, d'organiser et de configurer l'accès à vos données aux fins de répondre aux exigences spécifiques de votre entreprise, de votre organisation et de votre conformité.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Rubriques

- Fonctions d'Amazon S3
- Fonctionnement d'Amazon S3
- Modèle de cohérence des données Amazon S3
- Services connexes
- Accès à Amazon S3
- Paiement pour Amazon S3
- Conformité PCI DSS

Fonctions d'Amazon S3

Classes de stockage

Amazon S3 offre un large éventail de classes de stockage conçues pour différents cas d'utilisation. Par exemple, vous pouvez stocker les données de production stratégiques dans S3 Standard ou

S3 Express One Zone pour un accès fréquent, réduire les coûts en stockant les données rarement consultées dans S3 Standard-IA ou S3 One Zone-IA, et archiver les données à des coûts minimaux dans S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.

Amazon S3 Express One Zone est une classe de stockage Amazon S3 à zone unique et hautes performances, spécialement conçue pour fournir un accès aux données constant en moins de dix millisecondes pour vos applications les plus sensibles à la latence. S3 Express One Zone est la classe de stockage d'objets cloud qui présente la latence la plus faible à l'heure actuelle, avec une vitesse d'accès aux données jusqu'à 10 fois plus grande et des coûts de demande 50 % inférieurs à ceux de S3 Standard. S3 Express One Zone est la première classe de stockage S3 dans laquelle vous pouvez sélectionner une zone de disponibilité unique avec la possibilité de regrouper le stockage d'objets et les ressources de calcul, ce qui assure la vitesse d'accès la plus élevée possible. En outre, pour augmenter encore la vitesse d'accès et prendre en charge des centaines de milliers de demandes par seconde, les données sont stockées dans un nouveau type de compartiment : un compartiment de répertoires Amazon S3. Pour plus d'informations, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Vous pouvez stocker des données avec des modèles d'accès changeants ou inconnus dans S3 Intelligent-Tiering, ce qui optimise les coûts de stockage en déplaçant automatiquement vos données entre quatre niveaux d'accès lorsque vos modèles d'accès changent. Ces quatre niveaux d'accès comprennent deux niveaux d'accès à faible latence optimisés pour les accès fréquents et peu fréquents, et deux niveaux d'accès d'archive optionnels conçus pour un accès asynchrone pour les données rarement consultées.

Pour de plus amples informations, veuillez consulter Bien comprendre et gérer les classes de stockage Amazon S3.

Gestion du stockage

Amazon S3 dispose de fonctions de gestion du stockage que vous pouvez utiliser pour gérer les coûts, répondre aux exigences réglementaires, réduire la latence et enregistrer plusieurs copies distinctes de vos données aux fins de respecter les exigences de conformité.

- Cycle de vie S3 : configurez une configuration de cycle de vie pour gérer vos objets et les stocker de manière rentable pendant tout leur cycle de vie. Vous pouvez transférer des objets vers d'autres classes de stockage S3 ou faire expirer des objets qui atteignent la fin de leur durée de vie.
- Verrouillage d'objet S3 : empêchez que les objets Amazon S3 soient supprimés ou écrasés sur une période déterminée ou indéfinie. Vous pouvez utiliser Object Lock pour répondre aux exigences

réglementaires qui nécessitent un stockage write-once-read-many(WORM) ou simplement pour ajouter un niveau de protection supplémentaire contre les modifications et les suppressions d'objets.

- Réplication S3 : répliquez les objets ainsi que leurs métadonnées et balises d'objet respectives vers un ou plusieurs compartiments de destination identiques ou différents Régions AWS pour réduire la latence, la conformité, la sécurité et d'autres cas d'utilisation.
- Opérations par lots S3 – Gérez des milliards d'objets à grande échelle avec une seule demande API S3 ou quelques clics dans la console Amazon S3. Vous pouvez utiliser Batch Operations pour effectuer des opérations telles que Copy, Invoke AWS Lambda function et Restore sur des millions ou des milliards d'objets.

Gestion des accès et sécurité

Amazon S3 fournit des fonctions d'audit et de gestion de l'accès à vos compartiments et objets. Par défaut, les compartiments S3 et les objets sont privés. Vous avez uniquement accès aux ressources S3 que vous créez. Pour accorder des autorisations de ressources granulaires prenant en charge votre cas d'utilisation spécifique ou pour vérifier les autorisations de vos ressources Amazon S3, vous pouvez utiliser les fonctions suivantes.

- Bloquer l'accès public S3 – Bloque l'accès public aux compartiments S3 et aux objets. Par défaut, les paramètres de blocage de l'accès public sont activés au niveau du compartiment. Nous vous recommandons de laisser tous les paramètres de blocage de l'accès public activés, sauf si vous savez que vous devez en désactiver un ou plusieurs pour votre cas d'utilisation spécifique. Pour de plus amples informations, veuillez consulter Configuration des paramètres de blocage d'accès public pour vos compartiments S3.
- AWS Identity and Access Management (IAM) — IAM est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources, y compris à vos ressources Amazon S3. Avec IAM, vous pouvez gérer de manière centralisée les autorisations qui contrôlent les AWS ressources auxquelles les utilisateurs peuvent accéder. Vous pouvez utiliser IAM pour contrôler les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources.
- Politiques de compartiment – Utilisez un langage de politique basé sur IAM pour configurer les autorisations basées sur les ressources de vos compartiments S3 et des objets qu'ils contiennent.
- Amazon S3 access points (Points d'accès Amazon S3) — configurez des points de terminaison réseau nommés avec des stratégies d'accès dédiées pour gérer l'accès aux données à grande échelle pour les jeux de données partagés dans Amazon S3.

- Listes de contrôle d'accès (ACLs) : accordez des autorisations de lecture et d'écriture pour des compartiments et des objets individuels aux utilisateurs autorisés. En règle générale, nous recommandons d'utiliser des politiques basées sur les ressources S3 (politiques de compartiment et politiques de point d'accès) ou des politiques utilisateur IAM pour le contrôle d'accès au lieu de. ACLs Les politiques constituent une option de contrôle d'accès simplifiée et plus flexible. Les politiques de compartiment et de point d'accès vous permettent de définir des règles s'appliquant de manière générale à toutes les demandes adressées à vos ressources Amazon S3. Pour plus d'informations sur les cas spécifiques dans lesquels vous utiliseriez à la ACLs place des politiques basées sur les ressources ou des politiques utilisateur IAM, consultez. Gérer l'accès avec ACLs
- Propriété d'objets S3 : prenez possession de chaque objet présent dans votre compartiment, afin de simplifier la gestion des accès aux données stockées dans Amazon S3. La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour désactiver ou activer. ACLs Par défaut, ACLs sont désactivés. Lorsque cette option est ACLs désactivée, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès.
- Analyseur d'accès IAM pour S3 : évaluez et contrôlez vos politiques d'accès aux compartiments S3, en veillant à ce que ces politiques fournissent uniquement l'accès prévu à vos ressources S3.

Traitement des données

Pour transformer les données et déclencher des flux de travail afin d'automatiser diverses autres activités de traitement à grande échelle, vous pouvez utiliser les fonctions suivantes.

- S3 Object Lambda – ajoutez votre propre code aux requêtes S3 GET, HEAD et LIST afin de modifier et de traiter les données lorsqu'elles sont renvoyées vers une application. Filtrez les lignes, redimensionnez dynamiquement les images, supprimez les données confidentielles et bien plus encore.
- Notifications d'événements : déclenchez des flux de travail qui utilisent Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) et lorsqu'une modification AWS Lambda est apportée à vos ressources S3.

Journalisation et surveillance du stockage

Amazon S3 fournit des outils de journalisation et de surveillance que vous pouvez utiliser pour surveiller et contrôler la façon dont vos ressources Amazon S3 sont utilisées. Pour plus d'informations, consultez Outils de surveillance.

Outils de surveillance automatique

- Amazon CloudWatch Metrics for Amazon S3 — Suivez l'état de fonctionnement de vos ressources S3 et configurez des alertes de facturation lorsque les frais estimés atteignent un seuil défini par l'utilisateur.
- AWS CloudTrail— Enregistrez les actions effectuées par un utilisateur, un rôle ou un Service AWS dans Amazon S3. CloudTrail les journaux vous fournissent un suivi détaillé des API pour les opérations au niveau du bucket S3 et au niveau de l'objet.

Outils de surveillance manuelle

- La journalisation des accès au serveur fournit des enregistrements détaillés pour les demandes soumises à un compartiment. Vous pouvez utiliser les journaux d'accès au serveur pour des audits de sécurité et d'accès, afin d'en savoir plus sur votre base de clients et pour comprendre votre facture Amazon S3.
- AWS Trusted Advisor : évaluez votre compte à l'aide de vérifications des AWS meilleures pratiques pour identifier les moyens d'optimiser votre AWS infrastructure, d'améliorer la sécurité et les performances, de réduire les coûts et de surveiller les quotas de service. Vous pouvez ensuite suivre les recommandations pour optimiser vos services et vos ressources.

Analytique et informations

Amazon S3 offre des fonctions qui vous aident à gagner en visibilité sur l'utilisation de votre stockage, ce qui vous permet de mieux comprendre, analyser et optimiser votre stockage à grande échelle.

- Amazon S3 Storage Lens : comprenez, analysez et optimisez votre stockage. S3 Storage Lens fournit plus de 60 indicateurs d'utilisation et d'activité ainsi que des tableaux de bord interactifs pour agréger les données relatives à l'ensemble de votre organisation, à des comptes Régions AWS, à des compartiments ou à des préfixes spécifiques.
- Analyse de classe de stockage : analysez les modèles d'accès au stockage afin de décider lorsqu'il est temps de déplacer vos données vers une classe de stockage plus économique.
- Inventaire S3 avec rapports d'inventaire : auditez et produisez des rapports sur les objets et leurs métadonnées correspondantes, et configurez d'autres fonctions Amazon S3 pour qu'elles agissent dans les rapports d'inventaire. Par exemple, vous pouvez signaler le statut de réplication et de chiffrement de vos objets. Pour obtenir la liste de toutes les métadonnées disponibles pour chaque objet dans les rapports d'inventaire, consultez Liste d'inventaire Amazon S3.

Forte cohérence

Amazon S3 assure une forte read-after-write cohérence pour les requêtes PUT et DELETE relatives à l'ensemble des objets de votre compartiment Amazon S3 Régions AWS. Cela s'applique à la fois aux écritures sur de nouveaux objets ainsi qu'aux opérations PUT qui écrasent les objets existants et aux opérations DELETE. En outre, les opérations de lecture sur Amazon S3 Select, les listes de contrôle d'accès Amazon S3 (ACLs), les balises d'objets Amazon S3 et les métadonnées des objets (par exemple, l'objet HEAD) sont parfaitement cohérentes. Pour de plus amples informations, veuillez consulter Modèle de cohérence des données Amazon S3.

Fonctionnement d'Amazon S3

Amazon S3 est un service de stockage d'objets qui stocke les données sous forme d'objets, de données hiérarchiques ou de données tabulaires dans des compartiments. Un objet est un fichier et toutes les métadonnées qui le décrivent. Un compartiment est un conteneur d'objets.

Pour stocker vos données dans Amazon S3, vous devez d'abord créer un compartiment et spécifier un nom de compartiment et une Région AWS. Ensuite, vous chargez vos données dans ce compartiment en tant qu'objets dans Amazon S3. Chaque objet possède une key (clé) (ou key name [nom de clé]), qui est l'identifiant unique d'un objet au sein d'un compartiment.

S3 propose des fonctionnalités que vous pouvez configurer pour prendre en charge votre cas d'utilisation spécifique. Par exemple, vous pouvez utiliser la gestion des versions S3 pour conserver plusieurs versions d'un objet dans un même compartiment et vous permettre de restaurer des objets qui sont accidentellement supprimés ou écrasés.

Les compartiments et les objets qu'ils contiennent sont privés et ne sont accessibles que si vous accordez explicitement des autorisations d'accès. Vous pouvez utiliser des politiques de compartiment, des politiques AWS Identity and Access Management (IAM), des listes de contrôle d'accès (ACLs) et des points d'accès S3 pour gérer l'accès.

Rubriques

- Compartiments
- Objets
- Clés
- Gestion des versions S3

- ID de version
- Politique de compartiment
- Points d'accès S3
- Listes de contrôle d'accès (ACLs)
- Régions

Compartiments

Amazon S3 prend en charge quatre types de compartiments : les compartiments à usage général, les compartiments de répertoire, les compartiments de table et les compartiments vectoriels. Chaque type de compartiment fournit un ensemble unique de fonctionnalités pour différents cas d'utilisation.

Compartiments à usage général : les compartiments à usage général sont recommandés pour la plupart des cas d'utilisation et des modèles d'accès. Il s'agit du type de compartiment S3 d'origine. Un compartiment à usage général est un conteneur pour les objets stockés dans Amazon S3. Vous pouvez stocker autant d'objets que vous le souhaitez dans un compartiment et dans toutes les classes de stockage (à l'exception de S3 Express One Zone). Vous pouvez ainsi stocker des objets de manière redondante dans plusieurs zones de disponibilité. Pour plus d'informations, consultez Création, configuration et utilisation des compartiments à usage général Amazon S3.

> **Note**
>
> Par défaut, tous les compartiments à usage général sont privés. Toutefois, vous pouvez autoriser l'accès public à des buckets à usage général. Vous pouvez contrôler l'accès aux compartiments à usage général au niveau du bucket, du préfixe (dossier) ou de la balise d'objet. Pour plus d'informations, consultez la section Contrôle d'accès dans Amazon S3.

Buckets d'annuaire : recommandés pour les cas d'utilisation à faible latence et les cas d'utilisation liés à la résidence des données. Par défaut, vous pouvez créer jusqu'à 100 compartiments de répertoire dans votre répertoire Compte AWS, sans limite quant au nombre d'objets que vous pouvez stocker dans un compartiment de répertoire. Les compartiments de répertoire organisent les objets dans des répertoires hiérarchiques (préfixes) au lieu de la structure de stockage plate des compartiments à usage général. Ce type de compartiment ne comporte aucune limite de préfixe et les répertoires individuels peuvent être redimensionnés horizontalement. Pour plus d'informations, consultez la section Utilisation des compartiments de répertoire.

- Pour les cas d'utilisation à faible latence, vous pouvez créer un bucket d'annuaire dans une seule zone de AWS disponibilité pour stocker les données. Les compartiments de répertoires figurant dans des zones de disponibilité prennent en charge la classe de stockage S3 Express One Zone. Avec S3 Express One Zone, vos données sont stockées de façon redondante sur plusieurs appareils au sein d'une même zone de disponibilité. La classe de stockage S3 Express One Zone est recommandée si votre application est sensible aux performances et peut bénéficier d'une latence inférieure à dix millisecondes pour les demandes `PUT` et `GET`. Pour en savoir plus sur la création de compartiments d'annuaire dans les zones de disponibilité, consultez Charges de travail à hautes performances.
- Pour les cas d'utilisation liés à la résidence des données, vous pouvez créer un bucket de répertoire dans une seule zone locale AWS dédiée (DLZ) pour stocker les données. Dans les Zones Locales Dédiées, vous pouvez créer des compartiments d'S3annuaire pour stocker les données dans un périmètre de données spécifique, ce qui permet de prendre en charge vos cas d'utilisation liés à la résidence et à l'isolation des données. Les compartiments de répertoires des zones locales prennent en charge la classe de stockage S3 One Zone-Infrequent Access (S3 One Zone-IA ; Z-IA). Pour en savoir plus sur la création de compartiments de répertoires dans les Zones Locales, consultez la section Charges de travail liées à la résidence des données.

> **Note**
>
> L'accès public aux compartiments d'annuaire est désactivé par défaut. Ce comportement ne peut pas être modifié. Vous ne pouvez pas autoriser l'accès aux objets stockés dans des compartiments de répertoires. Vous pouvez accorder l'accès uniquement à vos compartiments de répertoires. Pour plus d'informations, consultez Authentification et autorisation des demandes.

Compartiments de tables : recommandés pour stocker des données tabulaires, telles que les transactions d'achat quotidiennes, les données de capteurs diffusées en continu ou les impressions publicitaires. Les données tabulaires représentent des données en colonnes et en lignes, comme dans une table de base de données. Les compartiments de tables fournissent un S3 stockage optimisé pour les charges de travail d'analyse et d'apprentissage automatique, avec des fonctionnalités conçues pour améliorer en permanence les performances des requêtes et réduire les coûts de stockage des tables. Les tables S3 sont spécialement conçues pour stocker des données tabulaires au format Apache Iceberg. Vous pouvez interroger des données tabulaires dans les tables S3 à l'aide des moteurs de requête populaires, notamment Amazon Athena Amazon Redshift, et

Apache Spark. Par défaut, vous pouvez créer jusqu'à 10 compartiments de tables Compte AWS par personne Région AWS et jusqu'à 10 000 tables par compartiment de table. Pour plus d'informations, consultez la section Utilisation des tables S3 et des compartiments de tables.

> **Note**
>
> Tous les compartiments de tables et toutes les tables sont privés et ne peuvent pas être rendus publics. Ces ressources sont accessibles uniquement par les utilisateurs auxquels l'accès a été accordé explicitement. Pour accorder l'accès, vous pouvez utiliser des politiques basées sur les ressources IAM pour les compartiments de tables et les tables, et des politiques basées sur l'identité IAM pour les utilisateurs et les rôles. Pour plus d'informations, consultez la section Sécurité des tables S3.

Compartiments vectoriels — Les compartiments vectoriels S3 sont un type de compartiment Amazon S3 spécialement conçu pour stocker et interroger des vecteurs. Les compartiments vectoriels utilisent des opérations d'API dédiées pour écrire et interroger des données vectorielles de manière efficace. Avec les compartiments vectoriels S3, vous pouvez stocker des intégrations vectorielles pour les modèles d'apprentissage automatique, effectuer des recherches de similarité et intégrer des services tels qu'Amazon Bedrock et Amazon. OpenSearch

Les compartiments vectoriels S3 organisent les données à l'aide d'index vectoriels, qui sont des ressources au sein d'un compartiment qui stockent et organisent les données vectorielles pour une recherche de similarité efficace. Chaque index vectoriel peut être configuré avec des dimensions, des mesures de distance (comme la similarité des cosinus) et des configurations de métadonnées spécifiques afin de l'optimiser pour votre cas d'utilisation spécifique. Pour de plus amples informations, veuillez consulter Utilisation de vecteurs S3 et de buckets vectoriels.

Informations supplémentaires sur tous les types de compartiments

Lorsque vous créez un compartiment, vous saisissez un nom de compartiment et choisissez la Région AWS où se trouve le compartiment. Une fois un compartiment créé, vous ne pouvez pas modifier son nom ni sa Région. Les noms des compartiments doivent respecter les règles de dénomination des compartiments suivantes :

- Règles de dénomination des compartiments à usage général
- Règles de dénomination des compartiments de répertoires
- Règles de dénomination des compartiments de tables

Les compartiments aussi :

- Organisez l'espace de noms Amazon S3 au niveau le plus élevé. Pour les buckets à usage général, cet espace de noms est. `S3` Pour les compartiments de répertoire, cet espace de noms est. `s3express` Pour les compartiments de table, cet espace de noms est. `s3tables`
- Identifiez le responsable de compte pour les frais de stockage et de transfert de données.
- Sert d'unité de regroupement pour les rapports d'utilisation.

Objets

Les objets sont les entités fondamentales stockées dans Amazon S3. Les objets sont composés de données et de métadonnées. Les métadonnées sont un ensemble de paires nom-valeur décrivant des objets. Ces pairs comprennent certaines métadonnées par défaut telles que la date de la dernière modification et des métadonnées HTTP standard comme `Content-Type`. Vous pouvez aussi spécifier des métadonnées personnalisées au moment du stockage de l'objet.

Chaque objet est contenu dans un compartiment. Par exemple, si l'objet nommé `photos/puppy.jpg` est stocké dans le compartiment à usage `amzn-s3-demo-bucket` général de la région de l'ouest des États-Unis (Oregon), il est adressable à l'aide de l'URL`https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`. Pour plus d'informations, consultez Accès à un compartiment.

Un objet est identifié de manière unique dans un compartiment par clé (nom) et un ID de version (si la gestion des versions S3 est activée sur le compartiment). Pour en savoir plus sur les objets, consultez Présentation des objets Amazon S3.

Clés

Une clé d'objet (ou nom de clé) est l'identifiant unique d'un objet au sein d'un compartiment. Chaque objet d'un compartiment possède une clé et une seule. La combinaison d'un compartiment, d'une clé d'objet et éventuellement d'un ID de version (si la gestion des versions S3 est activée pour le compartiment) identifie de manière unique chaque objet. Vous pouvez donc considérer Amazon S3 comme un mappage de données entre « compartiment + clé + version » et l'objet lui-même.

Chaque objet Amazon S3 peut être adressé de manière unique via la combinaison du point de terminaison du service web, du nom du compartiment, de la clé et, le cas échéant, d'une version. Par exemple, dans l'URL `https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/`

`photos/puppy.jpg`, « *`amzn-s3-demo-bucket`* » est le nom du compartiment et « `photos/puppy.jpg` » est la clé.

Pour en savoir plus sur les clés d'objet, consultez Attribution d'un nom aux objets Amazon S3.

Gestion des versions S3

Vous pouvez utiliser la gestion des versions S3 pour conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions S3 pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans vos compartiments. Vous pouvez facilement récupérer les données en cas d'actions involontaires des utilisateurs ou de défaillances des applications.

Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

ID de version

Lorsque vous activez la gestion des versions S3 pour un compartiment, Amazon S3 génère un ID de version unique pour chaque objet ajouté au compartiment. Les objets qui existaient déjà dans le compartiment au moment où vous activez la gestion des versions ont un ID de version égal à `null`. Si vous modifiez ces objets (ou tout autre) par d'autres opérations, telles que CopyObjectet PutObject, les nouveaux objets obtiennent un ID de version unique.

Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Politique de compartiment

Une politique de compartiment est une politique basée sur les ressources AWS Identity and Access Management (IAM) que vous pouvez utiliser pour accorder des autorisations d'accès à votre compartiment et aux objets qu'il contient. Seul le propriétaire du compartiment peut associer une politique à un compartiment. Les autorisations attachées au compartiment s'appliquent à tous les objets du compartiment appartenant au compte propriétaire du compartiment. Les politiques de compartiment sont limitées à une taille de 20 Ko.

Les politiques de compartiment utilisent le langage de politique d'accès basé sur JSON standard dans AWS. Vous pouvez utiliser des politiques de compartiment pour ajouter ou refuser des autorisations pour les objets d'un compartiment. Les politiques de compartiment autorisent ou rejettent les demandes basées sur les éléments de la stratégie, y compris le demandeur, les actions

S3, les ressources et les aspects ou conditions de la demande (par exemple, l'adresse IP utilisée pour effectuer la demande). Par exemple, vous pouvez créer une politique de compartiment qui accorde des autorisations entre comptes pour charger des objets vers un compartiment S3 tout en veillant à ce que le propriétaire du compartiment ait le contrôle total des objets téléchargés. Pour de plus amples informations, veuillez consulter Exemples de politiques de compartiment Amazon S3.

Dans votre politique de compartiment, vous pouvez utiliser des caractères génériques sur Amazon Resource Names (ARNs) et d'autres valeurs pour accorder des autorisations à un sous-ensemble d'objets. Par exemple, vous pouvez contrôler l'accès aux groupes d'objets qui commencent par un préfixecourant ou se terminent par une extension donnée, comme `.html`.

Points d'accès S3

Les points d'accès Amazon S3 sont appelés points de terminaison réseau dotés de politiques d'accès dédiées qui décrivent comment accéder aux données via ce point de terminaison. Les points d'accès sont attachés à une source de données sous-jacente, telle qu'un compartiment à usage général, un compartiment de répertoire ou un volume FSx pour OpenZFS, que vous pouvez utiliser pour effectuer des opérations sur des objets S3, telles que `GetObject` et. `PutObject` Les points d'accès simplifient la gestion de l'accès aux données à grande échelle pour les ensembles de données partagés dans Amazon S3.

Chaque point d'accès dispose de sa propre stratégie d'accès. Vous pouvez configurer les paramètres de blocage de l'accès public pour chaque point d'accès attaché à un bucket. Vous pouvez configurer n'importe quel point d'accès pour accepter uniquement les demandes provenant d'un cloud privé virtuel (VPC) afin de restreindre l'accès aux données Amazon S3 à un réseau privé.

Pour plus d'informations sur les points d'accès pour les buckets à usage général, consultezGestion de l'accès aux jeux de données avec des points d'accès . Pour plus d'informations sur les points d'accès pour les compartiments de répertoire, consultezGestion de l'accès aux ensembles de données partagés dans des compartiments d'annuaire dotés de points d'accès.

Listes de contrôle d'accès (ACLs)

Vous pouvez l'utiliser ACLs pour accorder des autorisations de lecture et d'écriture à des utilisateurs autorisés pour des buckets et des objets individuels à usage général. Chaque bucket ou objet à usage général est associé à une ACL en tant que sous-ressource. L'ACL définit le Comptes AWS ou les groupes auxquels l'accès est accordé et le type d'accès. ACLs sont un mécanisme de contrôle d'accès antérieur à l'IAM. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL).

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès à ceux-ci exclusivement à l'aide de politiques de gestion des accès.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Régions

Vous pouvez choisir la zone géographique Région AWS dans laquelle Amazon S3 stocke les buckets que vous créez. Vous pouvez choisir une Région pour optimiser la latence, minimiser les coûts ou répondre aux exigences réglementaires. Les objets stockés dans une région Région AWS ne quittent jamais la région, sauf si vous les transférez ou les répliquez explicitement dans une autre région. Par exemple, les objets stockés dans la Région Europe (Irlande) ne la quittent jamais.

> **Note**
>
> Vous pouvez accéder à Amazon S3 et à ses fonctionnalités uniquement dans Régions AWS les zones activées pour votre compte. Pour plus d'informations sur la façon de permettre à une région de créer et de gérer AWS des ressources, consultez Gérer Régions AWS dans le Références générales AWS.

Pour obtenir la liste des points de terminaison et des régions Amazon S3 disponibles, consultez Régions et points de terminaison dans la Références générales AWS.

Modèle de cohérence des données Amazon S3

Amazon S3 assure une forte read-after-write cohérence pour les requêtes PUT et DELETE relatives à l'ensemble des objets de votre compartiment Amazon S3 Régions AWS. Cela s'applique à la fois

aux écritures sur de nouveaux objets ainsi qu'aux demandes PUT qui écrasent les objets existants et aux demandes DELETE. En outre, les opérations de lecture sur Amazon S3 Select, les listes de contrôle d'accès Amazon S3 (ACLs), les balises d'objets Amazon S3 et les métadonnées des objets (par exemple, l'objet HEAD) sont parfaitement cohérentes.

Les mises à jour d'une seule clé sont atomiques. Par exemple, si vous faites une demande PUT sur une clé existante d'un thread et exécutez simultanément une demande GET sur la même clé à partir d'un second thread, vous obtiendrez les anciennes données ou les nouvelles données, mais jamais des données partielles ni corrompues.

Amazon S3 garantit une haute disponibilité en répliquant les données sur plusieurs serveurs dans les centres de données AWS . Si une demande PUT aboutit, vos données sont stockées en toute sécurité. Toute lecture (demandes GET ou LIST) initiée après la réception d'une réponse PUT réussie retournera les données écrites par la demande PUT. Voici des exemples de ce comportement :

- Un processus écrit un nouvel objet sur Amazon S3 et dresse immédiatement une liste des clés dans ce compartiment. Le nouvel objet s'affiche dans la liste.
- Un processus remplace un objet existant et tente immédiatement de le lire. Amazon S3 retourne les nouvelles données.
- Un processus efface un objet existant et tente immédiatement de le lire. Amazon S3 ne retourne aucune donnée, car l'objet a été supprimé.
- Un processus efface un objet existant et dresse immédiatement une liste des clés dans ce compartiment. L'objet ne s'affiche pas dans la liste.

> **Note**
>
> - Amazon S3 ne prend pas en charge le verrouillage d'objet pour les auteurs simultanés. Si deux demandes PUT sont effectuées simultanément sur la même clé, la demande indiquant l'horodatage le plus récent est retenue. Si cela pose un problème, vous devrez créer un mécanisme de verrouillage d'objet à votre application.
> - Les mises à jour sont basées sur les clés. Il n'est pas possible d'effectuer des mises à jour atomiques sur plusieurs clés. Par exemple, vous ne pouvez pas mettre à jour une clé qui dépend de la mise à jour d'une autre clé, sauf si vous intégrez cette fonctionnalité dans votre application.

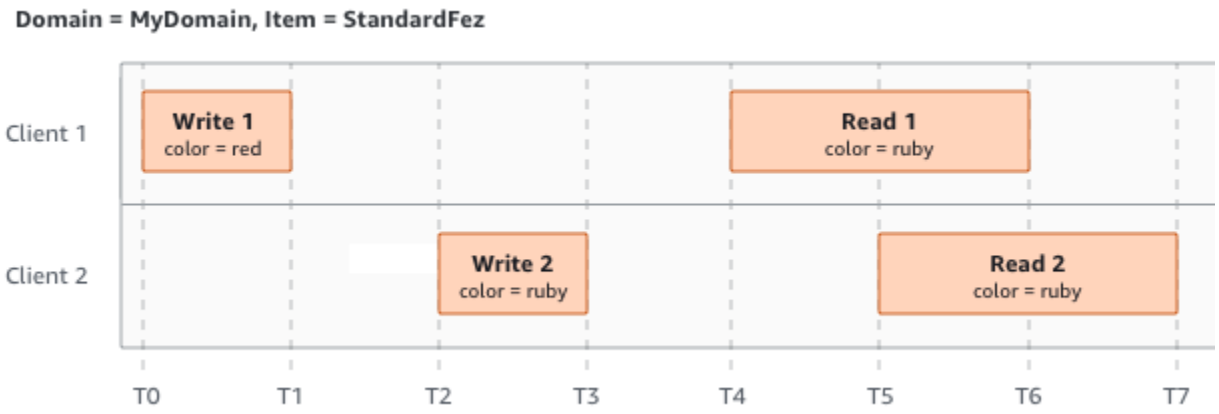
Les configurations de compartiment ont un modèle de cohérence éventuelle. Plus précisément, cela signifie que :

- Si vous supprimez un compartiment et répertoriez immédiatement tous les compartiments, il est possible que le compartiment supprimé figure toujours dans la liste.
- Si vous activez la gestion des versions sur un compartiment pour la première fois, la propagation complète de la modification peut prendre un court laps de temps. Nous vous recommandons d'attendre 15 minutes après l'activation de la gestion des versions avant d'exécuter des opérations d'écriture (demandes PUT ou DELETE) sur les objets du compartiment.

Applications simultanées

Cette section fournit des exemples de comportement à attendre de la part d'Amazon S3 lorsque plusieurs clients écrivent sur les mêmes éléments.

Dans cet exemple, W1 (écriture 1) et W2 (écriture 2) s'achèvent avant le début de R1 (lecture 1) et R2 (lecture 2). Comme S3 est fortement cohérent, R1 et R2 retournent tous les deux `color = ruby`.



Dans l'exemple suivant, W2 ne s'achève pas avant le début de R1. Par conséquent, R1 peut renvoyer `color = ruby` ou `color = garnet`. Cependant, puisque W1 et W2 se terminent avant le début de R2, R2 renvoie `color = garnet`.



Dans le dernier exemple, W2 commence avant que W1 ait reçu un accusé de réception. Par conséquent, ces écritures sont considérées comme simultanées. Amazon S3 utilise la last-writer-wins sémantique en interne pour déterminer quelle écriture est prioritaire. Toutefois, l'ordre dans lequel Amazon S3 reçoit les demandes et l'ordre dans lequel les applications reçoivent des accusés de réception ne peuvent pas être prédits en raison de différents facteurs, comme la latence réseau. Par exemple, W2 peut être initié par une EC2 instance Amazon dans la même région, tandis que W1 peut être initié par un hôte plus éloigné. La meilleure façon de déterminer la valeur finale consiste à effectuer la lecture une fois les deux écritures reconnues.



Services connexes

Après avoir chargé vos données dans Amazon S3, vous pouvez les utiliser avec d'autres AWS services. Les services suivants sont ceux que vous êtes susceptibles d'utiliser le plus fréquemment :

- Amazon Elastic Compute Cloud (Amazon EC2) — Fournit une capacité de calcul sécurisée et évolutive dans le AWS Cloud. Avec Amazon, vous EC2 n'avez plus besoin d'investir dans du

matériel dès le départ, ce qui vous permet de développer et de déployer des applications plus rapidement. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que nécessaire, configurer la sécurité et le réseau, et gérer le stockage.

- Amazon EMR : permet aux entreprises, aux chercheurs, aux analystes de données et aux développeurs de traiter de grandes quantités de données de manière simple et économique. Amazon EMR utilise un framework Hadoop hébergé qui s'exécute sur l'infrastructure Web d'Amazon et EC2 Amazon S3.
- AWS Snow Family : aide les clients qui ont besoin de gérer leurs opérations dans des environnements austères, autres que des centres de données, et dans des endroits où la connectivité réseau fait défaut. Vous pouvez utiliser les appareils AWS Snow Family pour accéder localement et à moindre coût au stockage et à la AWS Cloud puissance de calcul des appareils là où une connexion Internet n'est peut-être pas une option.
- AWS Transfer Family : fournit une prise en charge entièrement gérée des transferts de fichiers directement vers et depuis Amazon S3 ou Amazon Elastic File System (Amazon EFS) à l'aide du protocole File Transfer Protocol (SFTP) Secure Shell (SSH), du protocole File Transfer Protocol over SSL (FTPS) et du protocole File Transfer Protocol (FTP).

Accès à Amazon S3

Vous pouvez utiliser Amazon S3 de l'une des façons suivantes :

AWS Management Console

La console est une interface utilisateur Web permettant de gérer Amazon S3 et ses AWS ressources. Si vous vous êtes inscrit à un Compte AWS, vous pouvez accéder à la console Amazon S3 en vous connectant au AWS Management Console et en choisissant S3 sur la page d' AWS Management Console accueil.

AWS Command Line Interface

Vous pouvez utiliser les outils de ligne de AWS commande pour émettre des commandes ou créer des scripts sur la ligne de commande de votre système afin d'effectuer des tâches AWS (y compris S3).

Le AWS Command Line Interface (AWS CLI) fournit des commandes pour un large éventail de Services AWS. AWS CLI Il est pris en charge sur Windows, macOS et Linux. Consultez le

AWS Command Line Interface Guide de l'utilisateur pour démarrer. Pour plus d'informations sur les commandes d'Amazon S3, consultez les sections s3api et s3control dans la Référence des commandes de l'AWS CLI .

AWS SDKs

AWS fournit SDKs (kits de développement logiciel) composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Python, Ruby, .NET, iOS, Android, etc.). Ils AWS SDKs fournissent un moyen pratique de créer un accès programmatique à S3 et AWS. Amazon S3 est un service REST. Vous pouvez envoyer des demandes à Amazon S3 à l'aide des bibliothèques du AWS SDK, qui encapsulent l'API REST Amazon S3 sous-jacente et simplifient vos tâches de programmation. Par exemple, ils SDKs se chargent de tâches telles que le calcul des signatures, la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations sur les AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour AWS.

Chaque interaction avec Amazon S3 est authentifiée ou anonyme. Si vous utilisez le AWS SDKs, les bibliothèques calculent la signature pour l'authentification à partir des clés que vous fournissez. Pour plus d'informations sur la façon d'adresser des demandes à Amazon S3, consultez Envoi de demandes.

API REST Amazon S3

L'architecture d'Amazon S3 a été conçue de manière à être neutre en termes de langage de programmation et utilise nos interfaces supportées par AWS pour stocker et récupérer des objets. Vous pouvez accéder à S3 et à AWS par programmation à l'aide de l'API REST Amazon S3. L'API REST est une interface HTTP pour Amazon S3. Lorsque vous utilisez l'API REST, vous utilisez des demandes HTTP standard pour créer, récupérer et supprimer des compartiments et des objets.

Pour utiliser l'API REST, vous pouvez choisir n'importe quelle boîte à outils prenant en charge HTTP. Vous pouvez même utiliser un explorateur pour récupérer des objets, si ceux-ci peuvent être lus de manière anonyme.

L'API REST utilise les codes de statut et en-têtes HTTP standard afin de permettre aux explorateurs et boîtes à outils classiques de fonctionner. Dans certains zones, nous avons ajouté des fonctionnalités à HTTP (par exemple, nous avons ajouté des en-têtes afin de permettre le contrôle d'accès). Dans ces cas précis, nous avons fait notre possible pour intégrer cette nouvelle fonctionnalité de sorte qu'elle corresponde à la manière dont HTTP est généralement utilisé.

Si vous faites des appels directs d'API REST dans votre application, vous devez écrire le code pour calculer la signature et l'ajouter à la demande. Pour plus d'informations sur la façon d'adresser des demandes à Amazon S3, consultez Envoi de demandes dans la Référence d'API Amazon S3.

> **Note**
>
> Le support de l'API SOAP via HTTP est obsolète, mais continue d'être disponible sur HTTPS. Les nouvelles fonctions Amazon S3 ne sont pas prises en charge pour SOAP. Nous vous recommandons d'utiliser l'API REST ou le AWS SDKs.

Paiement pour Amazon S3

La tarification d'Amazon S3 est conçue de sorte que vous n'avez pas à planifier les besoins en stockage de votre application. La plupart des fournisseurs de stockage exigent que vous achetiez une quantité prédéterminée de capacité de stockage et de transfert réseau. Dans ce scénario, si vous dépassez cette capacité, votre service est fermé ou vous devez payer des coûts supplémentaires élevés. Si vous ne dépassez pas cette limite, vous payerez malgré tout comme si vous l'aviez pleinement utilisée.

Amazon S3 ne facture que ce que vous avez utilisé et il n'y a aucuns frais cachés ou supplémentaires. Ce modèle vous fournit un service à coût variable qui peut évoluer avec votre activité tout en vous offrant les avantages financiers de l'infrastructure. AWS Pour plus d'informations, consultez Tarification Amazon S3.

Lorsque vous vous inscrivez AWS, vous êtes automatiquement Compte AWS inscrit à tous les services AWS, y compris Amazon S3. Toutefois, seuls les services que vous utilisez vous sont facturés. Si vous êtes un nouveau client Amazon S3, vous pouvez commencer à utiliser Amazon S3 gratuitement. Pour plus d'informations, consultez la page sur l'offre gratuite AWS.

Pour consulter votre facture, dirigez-vous vers le Tableau de bord de gestion des coûts et de la facturation dans la AWS Billing and Cost Management console. Pour en savoir plus sur Compte AWS la facturation, consultez le guide de AWS Billing l'utilisateur. Si vous avez des questions concernant AWS la facturation Comptes AWS, contactez le AWS Support.

Conformité PCI DSS

Amazon S3 prend en charge le traitement, le stockage et la transmission des données de cartes bancaires par un commerçant ou un fournisseur de services et a été validé comme étant conforme à

la norme PCI (Payment Card Industry) DSS (Data Security Standard). Pour plus d'informations sur la norme PCI DSS, notamment sur la manière de demander une copie du Package de AWS conformité PCI, consultez la section PCI DSS niveau 1.

Premiers pas avec Amazon S3

Vous pouvez démarrer avec Amazon S3 en travaillant avec des compartiments et des objets. Un compartiment est un conteneur d'objets. Un objet est un fichier et toutes les métadonnées qui le décrivent.

Pour stocker un objet dans Amazon S3, vous créez un compartiment, puis téléchargez l'objet dans le compartiment. Lorsque l'objet se trouve dans le compartiment, vous pouvez l'ouvrir, le télécharger et le déplacer. Lorsque vous n'avez plus besoin d'un objet ou d'un compartiment, vous pouvez nettoyer vos ressources.

Avec Amazon S3, vous ne payez que les services que vous utilisez. Pour plus d'informations sur les fonctionnalités et les tarifs d'Amazon S3, consultez Amazon S3. Si vous êtes un nouveau client Amazon S3, vous pouvez commencer à utiliser Amazon S3 gratuitement. Pour plus d'informations, consultez la page sur l'offre gratuite AWS.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Vidéo : Premiers pas avec Amazon S3

Prérequis

Avant de commencer, confirmez que vous avez terminé les étapes de Configuration d'Amazon S3.

Configuration d'Amazon S3

Lorsque vous vous inscrivez AWS, vous êtes automatiquement Compte AWS inscrit à tous les services AWS, y compris Amazon S3. Seuls les services que vous utilisez vous sont facturés.

Avec Amazon S3, vous ne payez que les services que vous utilisez. Pour plus d'informations sur les fonctionnalités et les tarifs d'Amazon S3, consultez Amazon S3. Si vous êtes un nouveau client Amazon S3, vous pouvez commencer à utiliser Amazon S3 gratuitement. Pour plus d'informations, consultez la page sur l'offre gratuite AWS.

Pour configurer Amazon S3, suivez les étapes décrites dans les sections suivantes.

Lorsque vous vous inscrivez à Amazon S3 AWS et que vous le configurez, vous pouvez éventuellement modifier la langue d'affichage dans le AWS Management Console. Pour plus d'informations, consultez Modification de la langue de la AWS Management Console dans le Guide de démarrage de la AWS Management Console .

Rubriques

- Inscrivez-vous pour un Compte AWS
- Création d'un utilisateur doté d'un accès administratif

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Une partie de la procédure d'inscription consiste à recevoir un appel téléphonique ou un message texte et à saisir un code de vérification sur le clavier du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l'utilisateur racine a accès à l'ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l'utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Après vous être inscrit à un Compte AWS, sécurisez Utilisateur racine d'un compte AWS AWS IAM Identity Center, activez et créez un utilisateur administratif afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, voir Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

  Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .

2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Étape 1 : créer votre premier compartiment S3

Une fois inscrit AWS, vous êtes prêt à créer un compartiment dans Amazon S3 à l'aide du AWS Management Console. Dans Amazon S3, chaque objet est stocké dans un compartiment. Avant de pouvoir stocker des données dans Amazon S3, vous devez créer un compartiment.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

> **Note**
>
> Vous n'êtes pas facturé pour la création d'un compartiment. Seuls le stockage d'objets dans le compartiment et le transfert des objets dans et hors du compartiment vous sont facturés. Les frais que vous encourez en appliquant les exemples suivants de ce manuel sont minimes (moins de 1 USD). Pour plus d'informations sur les coûts de stockage, consultez Tarification Amazon S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.

> **Note**
>
> - Une fois le compartiment créé, vous ne pouvez pas changer sa région.
> - Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste d'Amazon S3 Régions AWS, consultez la section sur les Service AWS points de terminaison dans le Référence générale d'Amazon Web Services.

3. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
4. Choisissez Créer un compartiment. La page Créer un compartiment s'ouvre.
5. Pour Nom du compartiment, saisissez le nom de votre compartiment.

   Le nom du compartiment doit présenter les caractéristiques suivantes :

   - Être unique dans une partition. Une partition est un regroupement de régions. AWS possède actuellement trois partitions : `aws` (Régions commerciales), `aws-cn` (Régions de Chine) et `aws-us-gov` (AWS GovCloud (US) Regions).
   - Il doit comporter entre 3 et 63 caractères.
   - Composé uniquement de lettres minuscules, de chiffres, de points (`.`) et de traits d'union (). `-` Pour une compatibilité optimale, nous vous recommandons d'éviter d'utiliser des points (`.`) dans les noms de bucket, sauf pour les buckets utilisés uniquement pour l'hébergement de sites Web statiques.
   - Il doit commencer et se terminer par une lettre ou un chiffre.
   - Pour obtenir la liste complète des règles de dénomination des compartiments, consultez. Règles de dénomination des compartiments à usage général

   > **Important**
   >
   > - Une fois le compartiment créé, vous ne pouvez pas changer son nom.
   > - N'incluez pas d'informations sensibles dans le nom du bucket. Le nom du compartiment est visible en pointant vers les objets URLs qu'il contient.

6. (Facultatif) Sous Configuration générale, vous pouvez choisir de copier les paramètres d'un compartiment existant dans votre nouveau compartiment. Si vous ne souhaitez pas copier les paramètres d'un bucket existant, passez à l'étape suivante.

   > **Note**
   >
   > Cette option :
   >
   > - N'est pas disponible dans AWS CLI et n'est disponible que dans la console Amazon S3
   > - Ne copie pas la politique du bucket du bucket existant vers le nouveau bucket

   Pour copier les paramètres d'un compartiment existant, sous Copier les paramètres d'un compartiment existant, sélectionnez Choisir un compartiment. La fenêtre Choisir un compartiment s'ouvre. Recherchez le compartiment contenant les paramètres que vous souhaitez copier, puis sélectionnez Choisir un compartiment. La fenêtre Choisir un compartiment se ferme et la fenêtre Créer un compartiment s'ouvre à nouveau.

   Sous Copier les paramètres d'un bucket existant, vous pouvez désormais voir le nom du bucket que vous avez sélectionné. Les paramètres de votre nouveau compartiment correspondent désormais aux paramètres du compartiment que vous avez sélectionné. Si vous souhaitez supprimer les paramètres copiés, choisissez Restaurer les paramètres par défaut. Passez en revue les autres paramètres du bucket sur la page Créer un bucket. Si vous ne souhaitez apporter aucune modification, vous pouvez passer à l'étape finale.

7. Sous Propriété des objets, pour désactiver ou activer ACLs et contrôler la propriété des objets chargés dans votre bucket, sélectionnez l'un des paramètres suivants :

   ACLs handicapé

   - Application par le propriétaire du compartiment (par défaut) : ACLs cette option est désactivée, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment à usage général et en a le contrôle total. ACLs n'affectent plus les autorisations d'accès aux données du compartiment à usage général S3. Le compartiment utilise des stratégies exclusivement pour définir le contrôle des accès.

     Par défaut, ACLs sont désactivés. La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé,

sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

ACLs enabled

- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.

  Si vous appliquez le paramètre Propriétaire du compartiment préféré, pour exiger que tous les chargements Amazon S3 incluent la liste ACL prédéfinie `bucket-owner-full-control`, vous pouvez ajouter une politique de compartiment qui autorise uniquement les chargements d'objets utilisant cette liste ACL.
- Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

> **Note**
>
> Le paramètre par défaut est Propriétaire du compartiment appliqué. Pour appliquer le paramètre par défaut et le maintenir ACLs désactivé, seule l'`s3:CreateBucket`autorisation est nécessaire. Pour l'activer ACLs, vous devez avoir l'`s3:PutBucketOwnershipControls`autorisation.

8. Dans Paramètres de blocage de l'accès public pour ce compartiment, choisissez les paramètres Bloquer l'accès public que vous souhaitez appliquer au compartiment.

   Par défaut, les quatre paramètres de blocage de l'accès public sont activés. Nous vous recommandons de maintenir tous les paramètres activés, sauf si vous savez que vous devez en désactiver un ou plusieurs pour votre cas d'utilisation spécifique. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

> **Note**
>
> Pour activer tous les paramètres de blocage de l'accès public, seule l'autorisation `s3:CreateBucket` est requise. Pour désactiver les paramètres de blocage de l'accès public, vous devez disposer de l'autorisation `s3:PutBucketPublicAccessBlock`.

9. (Facultatif) Par défaut, le versionnement des compartiments est désactivé. La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans un même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment. Le contrôle de version permet de récupérer facilement les données en cas d'action involontaire d'un utilisateur ou de défaillance applicative. Pour plus d'informations sur la gestion des versions, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

   Pour activer le versionnement sur votre compartiment, choisissez Enable.

10. (Facultatif) Sous Tags (Balises), vous pouvez choisir d'ajouter des balises à votre compartiment. Avec la répartition des AWS coûts, vous pouvez utiliser des balises de compartiment pour annoter la facturation liée à l'utilisation d'un compartiment. Une balise correspond à une paire clé-valeur représentant un libellé que vous affectez à un compartiment. Pour de plus amples informations, veuillez consulter the section called "Utilisation des balises de répartition des coûts".

    Pour ajouter une balise de compartiment, saisissez une Key (Clé) et éventuellement une Value (Valeur), puis choisissez Add Tag (Ajouter une balise).

11. Pour configurer le chiffrement par défaut, sous Type de chiffrement, sélectionnez l'une des options suivantes :

    - Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
    - Chiffrement côté serveur avec AWS Key Management Service clés (SSE-KMS)
    - Chiffrement double couche côté serveur avec clés AWS Key Management Service (AWS KMS) (DSSE-KMS)

    > **Important**
    >
    > Si vous utilisez l'option SSE-KMS ou DSSE-KMS pour votre configuration de chiffrement par défaut, vous êtes soumis au quota de demandes par seconde (RPS) de. AWS KMS Pour plus d'informations sur les AWS KMS quotas et sur la manière de

demander une augmentation de quota, consultez la section Quotas dans le guide du AWS Key Management Service développeur.

Les buckets et les nouveaux objets sont chiffrés en utilisant le chiffrement côté serveur avec les clés gérées Amazon S3 (SSE-S3) comme niveau de base de configuration de chiffrement. Pour plus d'informations sur le chiffrement par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Pour en savoir plus sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

Pour plus d'informations sur l'utilisation du chiffrement côté serveur pour chiffrer vos données, consultez. the section called "Chiffrement des données"

12. Si vous avez choisi le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3) ou le chiffrement côté serveur double couche avec des clés () AWS Key Management Service (DSSE-KMS AWS KMS), procédez comme suit :

    a. Sous CléAWS KMS , spécifiez votre clé KMS de l'une des manières suivantes :

    - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans la liste des clés disponibles.

      La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

    - Pour saisir l'ARN de la clé KMS, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de votre clé KMS dans le champ qui s'affiche.
    - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

      Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS appartenant à un autre compte, vous devez d'abord être autorisé à utiliser la clé, puis saisir l'ARN de la clé KMS. Pour plus d'informations sur les autorisations entre comptes pour les clés KMS, consultez la section Création de clés KMS utilisables par d'autres comptes dans le guide du AWS Key Management Service développeur. Pour en savoir plus sur SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS). Pour en savoir plus sur DSSE-KMS, consultez the section called "Chiffrement double couche côté serveur (DSSE-KMS)".
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez Identification des clés KMS symétriques et asymétriques dans le Guide du développeur AWS Key Management Service .

b. Lorsque vous configurez votre compartiment pour utiliser le chiffrement par défaut avec SSE-KMS, vous pouvez également utiliser les clés de compartiment S3. Les clés de compartiment S3 réduisent le coût du chiffrement en diminuant le trafic de demandes d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3. Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS.

   Par défaut, les clés de compartiment S3 sont activées dans la console Amazon S3. Nous vous recommandons de laisser les clés de compartiment S3 activées pour réduire vos coûts. Pour désactiver les clés de compartiment S3 pour votre compartiment, sous Clé de compartiment, choisissez Disable.

13. (Facultatif) S3 Object Lock permet de protéger les nouveaux objets contre la suppression ou le remplacement. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la

fonctionnalité de verrouillage d'objet. Si vous souhaitez activer S3 Object Lock, procédez comme suit :

a. Choisissez Paramètres avancés.

> **Important**
>
> L'activation d'Object Lock active automatiquement le versionnement du bucket. Après avoir activé et créé le bucket avec succès, vous devez également configurer les paramètres de rétention par défaut et de conservation légale d'Object Lock dans l'onglet Propriétés du bucket.

b. Pour activer le verrouillage d'objets, choisissez Enable (Activer), lisez l'avertissement qui s'affiche et confirmez-le.

> **Note**
>
> Pour créer un bucket activé pour Object Lock, vous devez disposer des autorisations suivantes : `s3:CreateBuckets3:PutBucketVersioning`, `ets3:PutBucketObjectLockConfiguration`.

14. Choisissez Créer un compartiment.

Vous avez créé un compartiment dans Amazon S3.

Étape suivante

Pour ajouter un objet à votre compartiment, consultez Étape 2 : charger un objet dans votre compartiment.

Étape 2 : charger un objet dans votre compartiment

Après avoir créé un compartiment dans Amazon S3, vous êtes prêt à charger un objet dans celui-ci. Un objet peut désigner n'importe quel type de fichier : un fichier texte, une photo, une vidéo, etc.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Pour charger un objet dans un compartiment

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiment), choisissez le nom du compartiment dans lequel vous souhaitez charger votre objet.
3. Sous l'onglet Objets de votre compartiment, choisissez Charger.
4. Sous Fichiers et dossiers, choisissez Ajouter des fichiers.
5. Choisissez un fichier à charger, puis choisissez Ouvrir.
6. Choisissez Charger.

Vous avez réussi à charger un objet dans votre compartiment.

Étape suivante

Pour afficher votre objet, consultez Étape 3 : télécharger un objet.

Étape 3 : télécharger un objet

Lorsque vous chargez un objet dans un compartiment, vous pouvez afficher des informations sur votre objet et télécharger l'objet sur votre ordinateur local.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Utilisation de la console S3

Cette section explique comment utiliser la console Amazon S3 pour télécharger un objet depuis un compartiment S3.

> **Note**
>
> - Vous ne pouvez télécharger qu'un seul objet à la fois.
> - Si vous utilisez la console Amazon S3 pour télécharger un objet dont le nom de clé se termine par un point (`.`), celui-ci est supprimé du nom de clé de l'objet téléchargé. Pour conserver le délai à la fin du nom de l'objet téléchargé, vous devez utiliser l'API REST AWS Command Line Interface (AWS CLI) ou Amazon S3. AWS SDKs

Pour télécharger un objet à partir d'un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment à partir duquel vous souhaitez télécharger un objet.
4. Vous pouvez télécharger un objet à partir d'un compartiment S3 de l'une des façons suivantes :
   - Cochez la case à côté de l'objet et choisissez Télécharger. Si vous souhaitez télécharger l'objet dans un dossier spécifique, dans le menu Actions, choisissez Télécharger en tant que.
   - Si vous souhaitez télécharger une version spécifique de l'objet, activez Afficher les versions (en regard de la zone de recherche). Cochez la case à côté de la version de l'objet de votre choix, puis choisissez Télécharger. Si vous souhaitez télécharger l'objet dans un dossier spécifique, dans le menu Actions, choisissez Télécharger en tant que.

Vous avez téléchargé votre objet avec succès.

Étape suivante

Pour copier et coller votre objet dans Amazon S3, consultez Étape 4 : copier votre objet dans un dossier.

Étape 4 : copier votre objet dans un dossier

Vous avez déjà ajouté un objet dans un compartiment et téléchargé l'objet. Maintenant, vous créez un dossier et copiez l'objet et collez-le dans le dossier.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Pour copier un objet dans un dossier

1. Dans la liste Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Create folder (Créer un dossier) et configurez le nouveau dossier :
   a. Entrez un nom de dossier (par exemple, `favorite-pics`).
   b. Pour le paramètre de chiffrement du dossier, choisissez Désactiver.
   c. Choisissez Enregistrer.
3. Accédez au compartiment ou au dossier Amazon S3 contenant les objets que vous souhaitez copier.
4. Cochez la case située à gauche du nom des objets que vous souhaitez copier.
5. Choisissez Actions et Copy (Copier) dans la liste des options qui s'affiche.

   Vous pouvez également choisir Copy (Copier) parmi les options en haut à droite.
6. Choisissez le dossier de destination.
   a. Choisissez Parcourir S3.
   b. Cliquez sur le bouton d'option situé à gauche du nom du dossier.

      Pour naviguer dans un dossier et choisir un sous-dossier comme destination, choisissez le nom du dossier.
   c. Choisissez Choose destination (Choisir une destination).

Le chemin d'accès au dossier de destination apparaît dans la zone Destination. Dans Destination, vous pouvez également saisir votre chemin de destination, par exemple, s3 ://*bucket-name*//. *folder-name*

7. En bas à droite, choisissez Copy (Copier).

   Amazon S3 copie vos objets dans le dossier de destination.

Étape suivante

Pour supprimer un objet et un compartiment dans Amazon S3, consultez Étape 5 : supprimer vos objets et votre compartiment.

Étape 5 : supprimer vos objets et votre compartiment

Lorsque vous n'avez plus besoin d'un objet ou d'un compartiment, nous vous recommandons de les supprimer pour éviter des frais supplémentaires. Si vous avez terminé cette démonstration de démarrage en tant qu'exercice de formation et que vous ne prévoyez pas d'utiliser votre compartiment ou vos objets, nous recommandons de supprimer votre compartiment et vos objets afin que les frais ne s'accumulent plus.

Avant de supprimer votre compartiment, vous devez vider celui-ci ou supprimer les objets qui se trouvent dans le compartiment. Une fois que vous avez supprimé vos objets et votre compartiment, ils ne sont plus disponibles.

Si vous souhaitez continuer à utiliser le même nom de compartiment, nous vous recommandons de supprimer les objets ou de vider le compartiment, mais sans le supprimer. Une fois que vous avez supprimé un compartiment, le nom devient disponible et peut être réutilisé. Toutefois, un autre Compte AWS utilisateur peut créer un bucket portant le même nom avant que vous n'ayez la possibilité de le réutiliser.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Rubriques

- Suppression d'un objet
- Vider votre compartiment
- Suppression de votre compartiment

Suppression d'un objet

Si vous souhaitez choisir les objets que vous supprimez sans vider tous les objets de votre compartiment, vous pouvez supprimer un objet.

1. Dans la liste Compartiments, choisissez le nom du compartiment à partir duquel vous souhaitez supprimer un objet.
2. Sélectionnez l'objets que vous voulez supprimer.
3. Choisissez Supprimer dans les options affichées en haut à droite.
4. Sur la page Supprimer des objets, tapez **`delete`** pour confirmer la suppression de vos objets.
5. Choisissez Supprimer les objets.

Vider votre compartiment

Si vous envisagez de supprimer votre compartiment, vous devez d'abord vider celui-ci, ce qui supprimera tous les objets du compartiment.

Pour vider un compartiment :

1. Dans la liste Compartiments, sélectionnez le compartiment à vider, puis choisissez Vider.
2. Pour confirmer que vous souhaitez vider le compartiment et supprimer tous les objets qu'il contient, dans Empty bucket (Vider le compartiment), saisissez **`permanently delete`**.

   > **Important**
   >
   > Cette opération ne peut pas être annulée. Les objets ajoutés au compartiment pendant le vidage de celui-ci seront supprimés.

3. Pour vider le compartiment et supprimer tous les objets qu'il contient, choisissez Vider.

Une page Vider le compartiment : état s'ouvre et vous permet de consulter un résumé des suppressions d'objets qui ont réussi et échoué.

4. Pour revenir à votre liste de compartiments, choisissez Quitter.

Suppression de votre compartiment

Après avoir vidé votre compartiment ou supprimé tous les objets de votre compartiment, vous pouvez supprimer celui-ci.

1. Pour supprimer un compartiment, dans la liste Compartiments, sélectionnez le compartiment.
2. Choisissez Supprimer.
3. Pour confirmer la suppression, dans Delete bucket (Supprimer le compartiment), entrez le nom du compartiment.

> **Important**
>
> La suppression d'un compartiment ne peut pas être annulée. Les noms de compartiment sont uniques. Si vous supprimez votre bucket, un autre AWS utilisateur peut utiliser le nom. Si vous souhaitez continuer à utiliser le même nom de compartiment, ne supprimez pas le compartiment. Au lieu de cela, videz et conservez le compartiment.

4. Pour supprimer votre compartiment, choisissez Supprimer le compartiment.

Étapes suivantes

Dans les exemples précédents, vous avez appris à exécuter certaines tâches Amazon S3 élémentaires.

Les rubriques suivantes expliquent les chemins d'apprentissage que vous pouvez utiliser pour mieux comprendre Amazon S3 afin de pouvoir l'implémenter dans vos applications.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Rubriques

- Comprendre les cas d'utilisation courants
- Contrôlez l'accès à vos compartiments et à vos objets
- Protection et surveillance de votre stockage
- Développer avec Amazon S3
- Apprendre à partir de tutoriels
- Explorer la formation et le support

Comprendre les cas d'utilisation courants

Vous pouvez utiliser Amazon S3 pour prendre en charge votre cas d'utilisation particulier. La Bibliothèque de solutions AWS et le blog AWSfournissent des informations et des didacticiels propres au cas d'utilisation. Voici quelques cas d'utilisation courants d'Amazon S3 :

- Sauvegarde et stockage – Utilisez les fonctions de gestion du stockage Amazon S3 pour gérer les coûts, respecter les exigences réglementaires, réduire la latence et enregistrer plusieurs copies distinctes de vos données à des fins de respect des exigences de conformité.
- Hébergement d'applications – Déployez, installez et gérez des applications Web fiables, hautement évolutives et économiques. Par exemple, vous pouvez configurer votre compartiment Amazon S3 pour héberger un site web statique. Pour plus d'informations, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.
- Hébergement de contenus multimédias – Développez une infrastructure hautement disponible qui héberge des chargements et des téléchargements de vidéos, photos ou musique.
- Livraison de logiciels – Hébergez vos applications logicielles afin que vos clients puissent les télécharger.

Contrôlez l'accès à vos compartiments et à vos objets

Amazon S3 fournit plusieurs fonctionnalités et outils de sécurité. Pour avoir une présentation, consultez Contrôle d'accès dans Amazon S3.

Par défaut, les compartiments S3 et les objets sont privés. Vous avez uniquement accès aux ressources S3 que vous créez. Vous pouvez utiliser les fonctions suivantes pour accorder des autorisations de ressources granulaires qui prennent en charge votre cas d'utilisation particulier ou pour auditer les autorisations de vos ressources Amazon S3.

- Bloquer l'accès public S3 – Bloque l'accès public aux compartiments S3 et aux objets. Par défaut, les paramètres de blocage de l'accès public sont activés au niveau du compartiment.
- AWS Identity and Access Management Identités (IAM) — Utilisez IAM ou créez AWS IAM Identity Center des identités IAM Compte AWS pour gérer l'accès à vos ressources Amazon S3. Par exemple, vous pouvez utiliser IAM avec Amazon S3 pour contrôler le type d'accès d'un utilisateur ou d'un groupe d'utilisateurs à un compartiment Amazon S3 qui vous Compte AWS appartient. Pour obtenir plus d'informations sur les identités IAM et sur les bonnes pratiques, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles) dans le Guide de l'utilisateur IAM.
- Politiques de compartiment – Utilisez un langage de politique basé sur IAM pour configurer les autorisations basées sur les ressources de vos compartiments S3 et des objets qu'ils contiennent.
- Listes de contrôle d'accès (ACLs) : accordez des autorisations de lecture et d'écriture pour des compartiments et des objets individuels aux utilisateurs autorisés. En règle générale, nous recommandons d'utiliser des politiques basées sur les ressources S3 (politiques de compartiment et politiques de point d'accès) ou des politiques utilisateur IAM pour le contrôle d'accès au lieu de. ACLs Les politiques constituent une option de contrôle d'accès simplifiée et plus flexible. Les politiques de compartiment et de point d'accès vous permettent de définir des règles s'appliquant de manière générale à toutes les demandes adressées à vos ressources Amazon S3. Pour plus d'informations sur les cas spécifiques dans lesquels vous utiliseriez à la ACLs place des politiques basées sur les ressources ou des politiques utilisateur IAM, consultez. Gestion des identités et des accès pour Amazon S3
- Propriété d'objets S3 : prenez possession de chaque objet présent dans votre compartiment, afin de simplifier la gestion des accès aux données stockées dans Amazon S3. La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour désactiver ou activer. ACLs Par défaut, ACLs sont désactivés. Lorsque cette option est ACLs désactivée, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès.
- Analyseur d'accès IAM pour S3 : évaluez et contrôlez vos politiques d'accès aux compartiments S3, en veillant à ce que ces politiques fournissent uniquement l'accès prévu à vos ressources S3.

Protection et surveillance de votre stockage

- Protection de votre stockage : après avoir créé des compartiments et chargé des objets dans Amazon S3, vous pouvez protéger votre stockage d'objets. Par exemple, vous pouvez utiliser les contrôles de version S3, la réplication S3 et les contrôles de basculement des points d'accès multirégionaux pour la reprise après sinistre, AWS Backup pour sauvegarder vos données, et

S3 Object Lock pour définir les périodes de conservation, empêcher les suppressions et les remplacements, et répondre aux exigences de conformité.

- Surveillance de votre stockage : la surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon S3 et de vos AWS solutions. Vous pourrez surveiller l'activité et les coûts de stockage. En outre, nous vous recommandons de recueillir les données de surveillance de toutes les parties de votre solution AWS afin de pouvoir déboguer plus facilement une éventuelle défaillance à plusieurs points.

  Vous pouvez également utiliser l'analytique et les informations exploitables dans Amazon S3 pour comprendre, analyser et optimiser votre utilisation du stockage. Par exemple, utilisez Amazon S3 Storage Lens pour comprendre, analyser et optimiser votre stockage. S3 Storage Lens offre plus de 29 métriques d'utilisation et d'activité ainsi que des tableaux de bord interactifs vous permettant d'agréger des données pour l'ensemble de votre organisation, des comptes spécifiques, des Régions, des compartiments ou des préfixes. Utilisez Analyse de classe de stockage pour analyser les modèles d'accès au stockage afin de décider lorsqu'il est temps de déplacer vos données vers une classe de stockage plus économique. Pour gérer vos coûts, vous pouvez utiliser le cycle de vie S3.

Développer avec Amazon S3

Amazon S3 est un service REST. Vous pouvez envoyer des demandes à Amazon S3 à l'aide de l'API REST ou des bibliothèques du AWS SDK, qui encapsulent l'API REST Amazon S3 sous-jacente, simplifiant ainsi vos tâches de programmation. Vous pouvez également utiliser l' AWS Command Line Interface (AWS CLI) pour effectuer des appels d'API Amazon S3. Pour plus d'informations, consultez Envoi de demandes dans la Référence d'API Amazon S3.

L'API REST Amazon S3 est une interface HTTP vers Amazon S3. Lorsque vous utilisez l'API REST, vous utilisez des demandes HTTP standard pour créer, récupérer et supprimer des compartiments et des objets. Pour utiliser l'API REST, vous pouvez choisir n'importe quelle boîte à outils prenant en charge HTTP. Vous pouvez même utiliser un explorateur pour récupérer des objets, si ceux-ci peuvent être lus de manière anonyme. Pour plus d'informations, consultez Développement avec Amazon S3 dans la Référence d'API Amazon S3.

Pour vous aider à développer des applications utilisant le langage de votre choix, nous fournissons les ressources suivantes.

AWS CLI

Vous pouvez accéder aux fonctions d'Amazon S3 à l'aide de AWS CLI. Pour le télécharger et le configurer AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

AWS CLI Il fournit deux niveaux de commandes pour accéder à Amazon S3 : les commandes de haut niveau (s3) et les commandes au niveau de l'API (s3api et commandes). `s3control` Les commandes S3 de niveau élevé simplifient l'exécution des tâches courantes, telles que la création, la manipulation et la suppression d'objets et de compartiments. Les commandes s3api et s3control exposent l'accès direct à toutes les opérations d'API Amazon S3, que vous pouvez utiliser pour effectuer des opérations avancées qui pourraient ne pas être possibles avec les commandes de niveau élevé.

Pour obtenir la liste des AWS CLI commandes Amazon S3, consultez s3, s3api et s3control.

AWS SDKs et Explorers

Vous pouvez l'utiliser AWS SDKs lorsque vous développez des applications avec Amazon S3. AWS SDKs Simplifiez vos tâches de programmation en encapsulant l'API REST sous-jacente. Les JavaScript bibliothèques AWS Mobile SDKs et Amplify sont également disponibles pour créer des applications mobiles et Web connectées à l'aide de. AWS

En outre AWS SDKs, des AWS explorateurs sont disponibles pour Visual Studio et Eclipse pour Java IDE. Dans ce cas, les explorateurs SDKs et les explorateurs sont regroupés sous forme AWS de boîtes à outils.

Pour plus d'informations, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence des API Amazon S3.

Exemples de codes et bibliothèques

Le centre pour développeurs AWS et le catalogue d'exemples de codes AWS proposent des exemples de codes et des bibliothèques spécialement écrits pour Amazon S3. Vous pouvez utiliser ces exemples de codes afin de comprendre comment mettre en œuvre l'API Amazon S3. Vous pouvez également consulter la Référence des API Amazon Simple Storage Service pour comprendre les opérations de l'API Amazon S3 en détails.

Apprendre à partir de tutoriels

Vous pouvez commencer par des step-by-step didacticiels pour en savoir plus sur Amazon S3. Ces sont conçus pour un environnement de travaux pratiques et ils utilisent des noms de sociétés fictifs, des noms d'utilisateur fictifs, etc. Leur objectif consiste à fournir des instructions générales. Ils ne

sont pas conçus pour être utilisés directement dans votre environnement de production sans être préalablement vérifiés et adaptés soigneusement aux besoins uniques de votre organisation.

Premiers pas

- Tutoriel : stockage et récupération d'un fichier avec Amazon S3
- Tutoriel : démarrer avec Amazon S3 Intelligent-Tiering
- Tutoriel : démarrer avec les classes de stockage Amazon S3 Glacier

Optimisation des coûts de stockage

- Tutoriel : démarrer avec Amazon S3 Intelligent-Tiering
- Tutoriel : démarrer avec les classes de stockage Amazon S3 Glacier
- Tutoriel : optimisation des coûts et amélioration de la visibilité avec S3 Storage Lens

Gestion du stockage

- Didacticiel : Débuter à l'aide des points d'accès multi-régions Amazon S3
- Tutoriel : Réplication d'objets existants dans vos compartiments Amazon S3 avec la réplication par lot S3

Hébergement de vidéos et de sites web

- Tutoriel : Hébergement de vidéos en streaming à la demande avec Amazon S3 CloudFront, Amazon et Amazon Route 53
- Didacticiel : configuration d'un site web statique sur Amazon S3
- Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53

Traitement des données

- Didacticiel : Transformation de données pour votre application avec S3 Object Lambda
- Didacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend
- Tutoriel : Utilisation de S3 Object Lambda pour filigraner dynamiquement des images au fur et à mesure de leur récupération

- Didacticiel : transcodage par lot de vidéos avec les opérations par lot S3

Protection des données

- Tutoriel : vérifier l'intégrité des données dans Amazon S3 avec des totaux de contrôle supplémentaires
- Tutoriel : Réplication de données au sein et entre les deux à Régions AWS l'aide de S3 Replication
- Tutoriel : protection des données sur Amazon S3 contre les suppressions accidentelles ou les bogues d'application à l'aide de la gestion des versions S3, du verrouillage d'objets S3 et de la réplication S3
- Tutoriel : Réplication d'objets existants dans vos compartiments Amazon S3 avec la réplication par lot S3

Explorer la formation et le support

Vous pouvez apprendre auprès d' AWS experts pour améliorer vos compétences et obtenir l'assistance d'experts pour atteindre vos objectifs.

- Formation – Les ressources de formation offrent une approche pratique de l'apprentissage d'Amazon S3. Pour plus d'informations, consultez Formation et certification AWS et AWS online tech talks.
- Forums de discussion – Sur le forum, vous pouvez consulter des publications pour comprendre ce que vous pouvez faire ou non avec Amazon S3. Vous pouvez également poser des questions. Pour plus d'informations, consultez Forums de discussion.
- Assistance technique – Si vous avez d'autres questions, vous pouvez contacter l'Assistance technique.

Commencer à utiliser Amazon S3 à l'aide du AWS CLI

Vous pouvez commencer à utiliser Amazon S3 en utilisant le AWS Command Line Interface (AWS CLI) pour travailler avec des buckets et des objets à usage général. Un compartiment est un conteneur d'objets. Un objet est un fichier et toutes les métadonnées qui le décrivent.

Pour stocker un objet dans Amazon S3, vous créez un compartiment, puis téléchargez l'objet dans le compartiment. Lorsque l'objet se trouve dans le compartiment, vous pouvez l'ouvrir, le télécharger et

le déplacer. Lorsque vous n'avez plus besoin d'un objet ou d'un compartiment, vous pouvez nettoyer vos ressources.

Avec Amazon S3, vous ne payez que les services que vous utilisez. Pour plus d'informations sur les fonctionnalités et les tarifs d'Amazon S3, consultez Amazon S3. Si vous êtes un nouveau client Amazon S3, vous pouvez commencer à utiliser Amazon S3 gratuitement. Pour plus d'informations, consultez la page sur l'offre gratuite AWS.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez Didacticiel : bien démarrer avec S3 Express One Zone et Utilisation des compartiments de répertoires.

Configuration

Avant de commencer à utiliser le AWS CLI avec Amazon S3, assurez-vous que vous disposez des éléments suivants :

- J'ai ouvert un AWS compte. Pour obtenir des instructions, veuillez consulter Configuration d'Amazon S3.
- A créé un utilisateur avec `s3:*` des autorisations. Pour obtenir des instructions, veuillez consulter Configuration d'Amazon S3.
- A installé et configuré le AWS CLI. Pour obtenir des instructions, consultez Installation ou mise à jour de la dernière version de l' AWS CLI dans le Guide de l'utilisateur de l'AWS Command Line Interface .

Pour vérifier que le AWS CLI est correctement configuré, exécutez la commande suivante :

```
aws sts get-caller-identity
```

Pour plus d'informations, consultez get-caller-identity dans la Référence des commandes de l'AWS CLI .

Cette commande affiche la liste des commandes Amazon S3 disponibles si elles AWS CLI sont correctement installées et configurées.

Étape 1 : créer votre premier compartiment Amazon S3

Après avoir configuré le AWS CLI, vous êtes prêt à créer un compartiment dans Amazon S3. Dans Amazon S3, chaque objet est stocké dans un compartiment. Avant de pouvoir stocker des données dans Amazon S3, vous devez créer un compartiment.

> **Note**
>
> Vous n'êtes pas facturé pour la création d'un compartiment. Seuls le stockage d'objets dans le compartiment et le transfert des objets dans et hors du compartiment vous sont facturés. Les frais que vous encourez en appliquant les exemples suivants de ce manuel sont minimes (moins de 1 USD). Pour plus d'informations sur les coûts de stockage, consultez Tarification Amazon S3.

Pour créer un compartiment

1. Créez un bucket à l'aide de la `s3api create-bucket` commande. *`amzn-s3-demo-bucket`*Remplacez-le par un nom de compartiment unique et `us-east-1` par la région de votre choix :

   ```
   aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1
   ```

   Pour les régions autres que us-east-1, vous devez spécifier la contrainte de localisation :

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

   > **Note**
   >
   > - Une fois le compartiment créé, vous ne pouvez pas changer sa région.
   > - Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste des AWS régions Amazon S3, consultez la section Points AWS de terminaison de service dans le Référence générale d'Amazon Web Services.
   > - Le nom du compartiment doit présenter les caractéristiques suivantes :

- Être unique dans une partition. Une partition est un regroupement de régions. AWS possède actuellement trois partitions : `aws` (Régions commerciales), `aws-cn` (Régions de Chine) et `aws-us-gov` (AWS GovCloud (US) Régions).
- Il doit comporter entre 3 et 63 caractères.
- Composé uniquement de lettres minuscules, de chiffres, de points (.) et de tirets (-). Pour une compatibilité optimale, nous vous recommandons d'éviter d'utiliser des points (.) dans les noms de bucket, sauf pour les buckets utilisés uniquement pour l'hébergement de sites Web statiques.
- Il doit commencer et se terminer par une lettre ou un chiffre.

- Une fois le compartiment créé, vous ne pouvez pas changer son nom.
- N'incluez pas d'informations sensibles dans le nom du bucket. Le nom du compartiment est visible en pointant vers les objets URLs qu'il contient.

2. Vérifiez que votre compartiment a été créé en répertoriant tous les compartiments :

```
aws s3 ls
```

3. Pour la propriété des objets, vous pouvez désactiver ou activer ACLs et contrôler la propriété des objets chargés dans votre bucket.

   ACLs handicapé

   Pour que le propriétaire du bucket soit appliqué (par défaut), ACLs ils sont désactivés, et le propriétaire du bucket possède automatiquement tous les objets du bucket à usage général et en a le contrôle total :

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

   > **Note**
   >
   > Par défaut, ACLs sont désactivés. La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

ACLs activé

- Pour définir les préférences du propriétaire du bucket : le propriétaire du bucket possède et contrôle totalement les nouveaux objets que d'autres comptes écrivent dans le bucket avec l'ACL `bucket-owner-full-control` prédéfinie :

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=BucketOwnerPreferred}]"
```

  Si vous appliquez le paramètre préféré du propriétaire du compartiment et que vous souhaitez exiger que tous les téléchargements Amazon S3 incluent l'`bucket-owner-full-control`ACL prédéfinie, vous pouvez Exiger l' bucket-owner-full-controlACL prédéfini pour les PUT opérations Amazon S3 (préféré du propriétaire du compartiment) autoriser uniquement les téléchargements d'objets utilisant cette ACL.

- Pour configurer Object Writer : le AWS compte qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder via ACLs :

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-controls="Rules=[{ObjectOwnership=ObjectWriter}]"
```

> **Note**
>
> Le paramètre par défaut est Propriétaire du compartiment appliqué. Pour appliquer le paramètre par défaut et le maintenir ACLs désactivé, seule l'`s3:CreateBucket`autorisation est nécessaire. Pour l'activer ACLs, vous devez avoir l'`s3:PutBucketOwnershipControls`autorisation.

Pour vérifier le paramètre actuel de propriété de l'objet pour votre bucket :

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

4. Pour vérifier que le blocage de l'accès public est activé (il est activé par défaut pour les nouveaux compartiments) :

```
aws s3api get-public-access-block --bucket amzn-s3-demo-bucket
```

Par défaut, les quatre paramètres de blocage de l'accès public sont activés pour les nouveaux compartiments. Nous vous recommandons de maintenir tous les paramètres activés, sauf si vous savez que vous devez en désactiver un ou plusieurs pour votre cas d'utilisation spécifique. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

Si vous devez activer le blocage de l'accès public, utilisez la commande suivante :

```
aws s3api put-public-access-block --bucket amzn-s3-demo-bucket --public-access-
block-configuration
 "BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=t
```

> **Note**
>
> Pour activer tous les paramètres de blocage de l'accès public, seule l'autorisation `s3:CreateBucket` est requise. Pour désactiver les paramètres de blocage de l'accès public, vous devez disposer de l'autorisation `s3:PutBucketPublicAccessBlock`.

5. Pour activer le versionnement de votre bucket :

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket --versioning-
configuration Status=Enabled
```

Par défaut, la gestion des versions des compartiments est désactivée. La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans un même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment. Le contrôle de version permet de récupérer facilement les données en cas d'action involontaire d'un utilisateur ou de défaillance applicative. Pour plus d'informations sur la gestion des versions, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

6. Amazon S3 Object Lock permet de protéger les nouveaux objets contre la suppression ou le remplacement. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet. Pour l'activer Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet (nécessite la gestion des versions des compartiments) :

Pour un nouveau compartiment :

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket --region us-east-1 --object-lock-enabled-for-bucket
```

Pour un bucket existant :

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket --object-lock-configuration '{"ObjectLockEnabled": "Enabled"}'
```

Si vous souhaitez définir une valeur par défaut Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet tout en activant le verrouillage des objets, vous pouvez utiliser :

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket --object-lock-configuration '{"ObjectLockEnabled":"Enabled","Rule":{"DefaultRetention":{"Mode":"COMPLIANCE","Days":30}}}'
```

Vous pouvez le `"COMPLIANCE"` remplacer par `"GOVERNANCE"` pour un mode moins restrictif et ajuster le nombre de jours selon vos besoins.

> **Note**
>
> Pour créer un bucket activé pour Object Lock, vous devez disposer des autorisations suivantes : `s3:CreateBuckets3:PutBucketVersioning`, `ets3:PutBucketObjectLockConfiguration`.

7. Vous pouvez ajouter des balises à votre compartiment. Avec la répartition des AWS coûts, vous pouvez utiliser des balises de compartiment pour annoter la facturation liée à l'utilisation d'un compartiment. Une balise correspond à une paire clé-valeur représentant un libellé que vous affectez à un compartiment. Pour de plus amples informations, veuillez consulter Utilisation des balises de répartition des coûts pour les compartiments S3.

   Pour ajouter des tags à votre bucket :

   ```
   aws s3api put-bucket-tagging --bucket amzn-s3-demo-bucket --tagging
    'TagSet=[{Key=Purpose,Value=Testing},{Key=Environment,Value=Development}]'
   ```

8. Les compartiments et les nouveaux objets sont chiffrés à l'aide du chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base de configuration de chiffrement. Pour vérifier le chiffrement par défaut de votre bucket, utilisez la commande suivante :

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket
```

Vous pouvez également configurer le chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) et le chiffrement double couche côté serveur avec des AWS KMS clés (DSSE-KMS) pour votre compartiment. La clé AWS gérée (aws/s3) et les clés gérées par le client peuvent être utilisées comme clé SSE-KMS et comme AWS KMS clé pour la configuration du DSSE-KMS chiffrement. Pour plus d'informations sur les clés gérées par le client, consultez la section Clés et AWS clés client dans le Guide du AWS Key Management Service développeur. Pour plus d'informations sur la création d'une AWS KMS clé, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> La AWS KMS clé doit se trouver dans la même AWS région que votre compartiment Amazon S3. Les clés KMS entre régions ne sont pas prises en charge pour le chiffrement des compartiments Amazon S3.

Lorsque vous configurez votre compartiment pour utiliser le chiffrement par défaut avec SSE-KMS, vous pouvez également utiliser les clés de compartiment Amazon S3. Les clés de compartiment Amazon S3 réduisent le coût du chiffrement en diminuant le trafic de demandes provenant d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3. Les clés de compartiment Amazon S3 ne sont pas prises en charge pour le DSSE-KMS. Dans le AWS CLI, les clés de compartiment Amazon S3 NE sont PAS activées par défaut lors de la création d'un nouveau compartiment. Ce comportement est différent du comportement de la console où ils sont activés par défaut.

Pour configurer SSE-KMS et activer les clés de compartiment Amazon S3 :

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-
encryption-configuration "{\"Rules\":[{\"ApplyServerSideEncryptionByDefault
```

```
\":{\"SSEAlgorithm\":\"aws:kms\",\"KMSMasterKeyID\":\"YOUR-KMS-KEY-ARN\"},
\"BucketKeyEnabled\":true}]}"
```

Pour vérifier si les clés de compartiment Amazon S3 sont activées pour un compartiment :

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket
```

La sortie inclura un `BucketKeyEnabled` champ défini sur `true` ou`false`.

Pour configurer`DSSE-KMS`, utilisez la commande suivante :

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-
encryption-configuration '{"Rules":[{"ApplyServerSideEncryptionByDefault":
{"SSEAlgorithm":"aws:kms:dsse","KMSMasterKeyID":"YOUR-KMS-KEY-ARN"}}]}'
```

Pour plus d'informations sur le chiffrement par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Pour en savoir plus sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

> **Important**
>
> Si vous utilisez l'option SSE-KMS ou DSSE-KMS pour votre configuration de chiffrement par défaut, vous êtes soumis au quota de demandes par seconde (RPS) de. AWS KMS Vous pouvez réduire les appels d'API KMS en activant les clés de compartiment Amazon S3, ce qui réduit le nombre de demandes envoyées à AWS KMS. Pour plus d'informations sur les quotas de AWS KMS et sur la procédure à suivre pour demander une augmentation des quotas, consultez Quotas dans le Guide du développeur AWS Key Management Service .

Vous avez créé un compartiment dans Amazon S3. L'étape suivante consiste à télécharger un objet dans votre compartiment.

Étape 2 : charger un objet dans votre compartiment

Après avoir créé un compartiment dans Amazon S3, vous êtes prêt à charger un objet dans celui-ci. Un objet peut désigner n'importe quel type de fichier : un fichier texte, une photo, une vidéo, etc.

Pour charger un objet dans un compartiment

1. Créez un simple fichier texte à télécharger. Vous pouvez utiliser n'importe quel éditeur de texte ou exécuter la commande suivante :

   ```
   echo 'Hello, Amazon S3!' > example.txt
   ```

2. Téléchargez le fichier dans votre compartiment à l'aide de la commande s3 cp :

   ```
   aws s3 cp example.txt s3://amzn-s3-demo-bucket/
   ```

   Si le téléchargement est réussi, vous verrez un résultat similaire à :

   ```
   upload: ./example.txt to s3://amzn-s3-demo-bucket/example.txt
   ```

3. Vérifiez que l'objet a été chargé en répertoriant le contenu de votre compartiment :

   ```
   aws s3 ls s3://amzn-s3-demo-bucket/
   ```

Vous avez réussi à charger un objet dans votre compartiment. L'étape suivante consiste à télécharger un objet.

Étape 3 : télécharger un objet

Lorsque vous chargez un objet dans un compartiment, vous pouvez afficher des informations sur votre objet et télécharger l'objet sur votre ordinateur local.

Pour télécharger un objet depuis un compartiment Amazon S3

1. Pour obtenir des informations sur votre objet :

   ```
   aws s3api head-object --bucket amzn-s3-demo-bucket --key example.txt
   ```

   Cette commande renvoie des métadonnées relatives à l'objet, notamment son type de contenu, sa longueur et sa date de dernière modification.

2. Téléchargez l'objet sur votre ordinateur local :

   ```
   aws s3 cp s3://amzn-s3-demo-bucket/example.txt downloaded-example.txt
   ```

Si le téléchargement est réussi, vous verrez un résultat similaire à :

```
download: s3://amzn-s3-demo-bucket/example.txt to ./downloaded-example.txt
```

3. Vérifiez le contenu du fichier téléchargé :

```
cat downloaded-example.txt
```

> **Note**
>
> - Contrairement à la console, elle AWS CLI peut télécharger plusieurs objets à la fois en utilisant des caractères génériques ou le `--recursive` drapeau.
> - Lorsque vous téléchargez des objets avec le AWS CLI point (.) à la fin du nom des clés d'objet, ils sont conservés, contrairement à ce qui se passe dans la console où ils sont supprimés. C'est important si vos clés d'objet se terminent par des points.

Exemple de téléchargement de plusieurs objets :

Pour télécharger plusieurs objets depuis un compartiment Amazon S3 avec des extensions de fichier spécifiques, utilisez la commande de copie récursive avec `exclude` et `include` filtres, comme indiqué dans l'exemple.

```
aws s3 cp s3://amzn-s3-demo-bucket/ . --recursive --exclude "*" --include "*.txt"
```

Vous avez téléchargé votre objet avec succès. L'étape suivante consiste à copier votre objet dans un dossier.

Étape 4 : copier votre objet dans un dossier

Vous avez déjà ajouté un objet dans un compartiment et téléchargé l'objet. À présent, vous devez créer un dossier et y copier l'objet.

Pour copier un objet dans un dossier

1. Dans Amazon S3, les dossiers sont représentés par des préfixes dans les clés d'objet. Créez un « dossier » en copiant un objet avec un préfixe :

```
aws s3 cp s3://amzn-s3-demo-source-bucket/example.txt s3://amzn-s3-demo-destination-bucket/favorite-files/example.txt
```

Si la copie est réussie, vous obtiendrez un résultat similaire à :

```
copy: s3://amzn-s3-demo-source-bucket/example.txt to s3://amzn-s3-demo-destination-bucket/favorite-files/example.txt
```

2. Vérifiez que l'objet a été copié en répertoriant le contenu du dossier :

```
aws s3 ls s3://amzn-s3-demo-destination-bucket/favorite-files/
```

Vous avez correctement copié votre objet dans un dossier. L'étape suivante consiste à supprimer vos objets et votre bucket.

Étape 5 : supprimer vos objets et votre compartiment

Lorsque vous n'avez plus besoin d'un objet ou d'un compartiment, nous vous recommandons de les supprimer pour éviter des frais supplémentaires. Si vous avez terminé cette démonstration de démarrage en tant qu'exercice de formation et que vous ne prévoyez pas d'utiliser votre compartiment ou vos objets, nous recommandons de supprimer votre compartiment et vos objets afin que les frais ne s'accumulent plus.

Avant de supprimer votre compartiment, vous devez vider celui-ci ou supprimer les objets qui se trouvent dans le compartiment. Une fois que vous avez supprimé vos objets et votre compartiment, ils ne sont plus disponibles.

Si vous souhaitez continuer à utiliser le même nom de compartiment, nous vous recommandons de supprimer les objets ou de vider le compartiment, mais sans le supprimer. Une fois que vous avez supprimé un compartiment, le nom devient disponible et peut être réutilisé. Toutefois, un autre AWS compte peut créer un bucket portant le même nom avant que vous ne puissiez le réutiliser.

Suppression d'un objet

Si vous souhaitez choisir les objets que vous supprimez sans vider tous les objets de votre compartiment, vous pouvez supprimer un objet.

Supprimer un objet spécifique :

```
aws s3 rm s3://amzn-s3-demo-bucket/example.txt
```

Si la suppression est réussie, vous verrez un résultat similaire à :

```
delete: s3://amzn-s3-demo-bucket/example.txt
```

Vider votre compartiment

Si vous envisagez de supprimer votre compartiment, vous devez d'abord le vider, ce qui supprime tous les objets, toutes les versions et tous les marqueurs de suppression qu'il contient.

Pour vider un compartiment :

> **Important**
>
> Cette opération ne peut pas être annulée. Les objets ajoutés au compartiment pendant le vidage de celui-ci seront supprimés.

1. Option 1 : pour les petits compartiments, utilisez la `rm` commande avec l'`--recursive`indicateur pour supprimer tous les objets du compartiment :

   ```
   aws s3 rm s3://amzn-s3-demo-bucket --recursive
   ```

   Cette commande supprime tous les objets du compartiment, y compris les objets des dossiers.

   > **Note**
   >
   > Si votre compartiment contient de nombreux objets ou des objets de grande taille, le délai de cette commande peut être dépassé. Pour les compartiments contenant de grandes quantités de données, utilisez la règle Amazon S3 Lifecycle pour faire expirer les objets contenus dans les compartiments.

   Option 2 : utiliser les règles du cycle de vie d'Amazon S3 (recommandé pour les grands compartiments)

Pour les buckets contenant de nombreux objets ou des objets volumineux, utilisez une règle Amazon S3 Lifecycle pour expirer et supprimer automatiquement tous les objets. Attendez que la règle du cycle de vie soit traitée (cela peut prendre jusqu'à 24 heures). Pour plus d'informations sur l'utilisation de règles de cycle de vie pour vider des compartiments, consultez Comment vider un compartiment Amazon S3 à l'aide d'une règle de configuration du cycle de vie ? .

2. Vérifiez que le compartiment est vide :

```
aws s3 ls s3://amzn-s3-demo-bucket
```

3. Si le contrôle de version est activé dans votre compartiment, utilisez les commandes suivantes pour supprimer les objets versionnés et supprimer les marqueurs.

   Supprimer les objets versionnés :

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete "$(aws s3api list-
object-versions --bucket amzn-s3-demo-bucket --output json --query='{Objects:
 Versions[].{Key:Key,VersionId:VersionId}}')"
```

   Supprimez les marqueurs de suppression :

```
aws s3api delete-objects --bucket amzn-s3-demo-bucket --delete "$(aws s3api list-
object-versions --bucket amzn-s3-demo-bucket --output json --query='{Objects:
 DeleteMarkers[].{Key:Key,VersionId:VersionId}}')"
```

4. Vérifiez que toutes les versions de l'objet sont vides dans le compartiment et supprimez les marqueurs :

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket
```

   La sortie ne doit afficher aucune version ou supprimer les marqueurs restants.

Suppression de votre compartiment

Après avoir vidé votre compartiment ou supprimé tous les objets de votre compartiment, vous pouvez supprimer celui-ci.

> **Important**
>
> La suppression d'un bucket est irréversible. Les noms de compartiment sont uniques. Si vous supprimez votre bucket, un autre AWS utilisateur peut utiliser le nom. Si vous souhaitez continuer à utiliser le même nom de compartiment, ne supprimez pas le compartiment. Au lieu de cela, videz et conservez le compartiment.

Pour supprimer votre bucket

1. Supprimez votre compartiment :

```
aws s3api delete-bucket --bucket amzn-s3-demo-bucket
```

2. Vérifiez que le bucket a été supprimé en listant tous vos buckets :

```
aws s3 ls
```

Étapes suivantes

Dans les exemples précédents, vous avez appris à effectuer certaines tâches de base d'Amazon S3 à l'aide du AWS CLI.

Les rubriques suivantes expliquent les chemins d'apprentissage que vous pouvez utiliser pour mieux comprendre Amazon S3 afin de pouvoir l'implémenter dans vos applications.

- Comprendre les cas d'utilisation courants
- Contrôlez l'accès à vos compartiments et à vos objets
- Protection et surveillance de votre stockage
- Développer avec Amazon S3
- Comprendre les cas d'utilisation courants
- Explorer la formation et le support

La liste suivante présente AWS CLI les commandes courantes pour Amazon S3 :

- cp — Copie des fichiers ou des objets entre votre système de fichiers local et Amazon S3, ou entre des emplacements Amazon S3

- ls — Répertorie les objets Amazon S3 et les préfixes courants sous un compartiment et un préfixe spécifiés
- mb — Crée un compartiment Amazon S3
- mv — Déplace des fichiers ou des objets entre votre système de fichiers local et Amazon S3, ou entre des emplacements Amazon S3
- presign — Génère une URL pré-signée pour un objet Amazon S3 qui autorise un accès temporaire sans informations d'identification AWS
- rb — Supprime un compartiment Amazon S3 vide. Vous pouvez utiliser l'`--force`indicateur pour vider et supprimer automatiquement un compartiment contenant son contenu en une seule commande. Cette action ne peut pas être annulée.
- rm — Supprime des objets d'Amazon S3
- sync — Synchronise les répertoires et les préfixes Amazon S3 en copiant de manière récursive les fichiers nouveaux et mis à jour du répertoire source vers la destination.
- site web — Configure un bucket en tant que site Web statique

Pour plus d'informations sur les AWS CLI commandes pour Amazon S3, consultez les ressources suivantes :

- s3 — Commandes Amazon S3 de haut niveau qui simplifient les opérations courantes
- s3api — Accès direct à toutes les opérations de l'API Amazon S3
- s3control — Accès direct à toutes les opérations de l'API Amazon S3 Control

Création, configuration et utilisation de compartiments à usage général Amazon S3

Pour stocker vos données dans Amazon S3, vous devez utiliser avec des ressources appelées compartiments et objets. Un compartiment est un conteneur d'objets. Un objet est un fichier et toutes les métadonnées qui le décrivent.

Pour stocker un objet dans Amazon S3, vous devez créer un compartiment, puis télécharger l'objet dans un compartiment. Lorsque l'objet se trouve dans le compartiment, vous pouvez l'ouvrir, le télécharger et le déplacer. Lorsque vous n'avez plus besoin d'un objet ou d'un compartiment, vous pouvez nettoyer vos ressources.

Les rubriques de cette section fournissent une vue d'ensemble de l'utilisation des compartiments à usage général dans Amazon S3. Ils incluent des informations sur la dénomination, la création, l'accès et la suppression de compartiments à usage général. Pour plus d'informations sur l'affichage ou l'établissement de la liste des objets d'un compartiment, consultez Organisation, liste et utilisation de vos objets.

Il existe plusieurs types de compartiments Amazon S3. Avant de créer un bucket, assurez-vous de choisir le type de bucket qui correspond le mieux à votre application et à vos exigences de performance. Pour plus d'informations sur les différents types de bucket et les cas d'utilisation appropriés pour chacun, consultezCompartiments.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

> **Note**
>
> Avec Amazon S3, vous ne payez que les services que vous utilisez. Pour plus d'informations sur les fonctionnalités et les tarifs d'Amazon S3, consultez Amazon S3. Si vous êtes un nouveau client Amazon S3, vous pouvez commencer à utiliser Amazon S3 gratuitement. Pour plus d'informations, consultez la page sur l'offre gratuite AWS.

Rubriques

- Présentation des compartiments à usage général
- Modèles de compartiments à usage général courants pour créer des applications sur Amazon S3
- Règles de dénomination des compartiments à usage général
- Quotas, limites et restrictions relatifs aux compartiments à usage général
- Accès à un compartiment à usage général Amazon S3
- Création d'un bucket à usage général
- Afficher les propriétés d'un bucket S3 à usage général
- Répertorier les compartiments à usage général d'Amazon S3
- Vidange d'un seau à usage général
- Supprimer un bucket à usage général
- Monter un compartiment Amazon S3 en tant que système de fichiers local
- Utilisation du navigateur de stockage pour Amazon S3
- Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration
- Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation

Présentation des compartiments à usage général

Pour charger vos données (photos, vidéos, documents, etc.) dans Amazon S3, vous devez d'abord créer un compartiment S3 dans l'une des Régions AWS.

Il existe plusieurs types de compartiments Amazon S3. Avant de créer un bucket, assurez-vous de choisir le type de bucket qui correspond le mieux à votre application et à vos exigences de performance. Pour plus d'informations sur les différents types de bucket et les cas d'utilisation appropriés pour chacun, consultezCompartiments.

Les sections suivantes fournissent des informations supplémentaires sur les compartiments à usage général, notamment les règles de dénomination, les quotas et les détails de configuration des compartiments. Pour obtenir la liste des restrictions et limitations relatives aux compartiments Amazon S3, consultez Quotas, limites et restrictions relatifs aux compartiments à usage général.

Rubriques

- Présentation des compartiments à usage général
- Modèles de seaux à usage général courants
- Autorisations
- Gestion de l'accès du public aux compartiments à usage général
- Options de configuration des buckets à usage général
- Fonctionnement des godets à usage général
- Surveillance des performances des godets à usage général

Présentation des compartiments à usage général

Chaque objet est contenu dans un compartiment. Par exemple, si l'objet nommé `photos/puppy.jpg` est stocké dans le compartiment à usage `amzn-s3-demo-bucket` général de la région de l'ouest des États-Unis (Oregon), il est adressable à l'aide de l'URL`https://amzn-s3-demo-bucket.s3.us-west-2.amazonaws.com/photos/puppy.jpg`. Pour plus d'informations, consultez Accès à un compartiment.

- Les quotas de compartiments à usage général pour les régions commerciales ne peuvent être consultés et gérés qu'à partir de la région USA Est (Virginie du Nord).
- Les quotas de bucket à usage général pour ne AWS GovCloud (US) peuvent être consultés et gérés qu'à partir de AWS GovCloud (US-West).

En termes de mise en œuvre, les buckets et les objets sont AWS des ressources, et Amazon S3 vous permet APIs de les gérer. Par exemple, vous pouvez créer un compartiment et y charger des objets via l'API Amazon S3. Vous pouvez également effectuer ces opérations via la console Amazon S3. La console utilise Amazon S3 APIs pour envoyer des demandes à Amazon S3.

Cette section explique comment utiliser des buckets à usage général. Pour en savoir plus sur l'utilisation des objets, consultez Présentation des objets Amazon S3.

Amazon S3 prend en charge les compartiments universels à usage général, ce qui signifie que chaque nom de compartiment doit être unique pour Comptes AWS l'ensemble de Régions AWS la partition. Une partition est un regroupement de régions. AWS possède actuellement trois partitions : `aws` (Régions standard), `aws-cn` (Régions de Chine) et `aws-us-gov` (AWS GovCloud (US)).

Une fois qu'un bucket à usage général est créé, le nom de ce bucket ne peut pas être utilisé par un autre utilisateur Compte AWS de la même partition tant que le bucket n'est pas supprimé. Vous

ne devez pas dépendre de conventions de dénomination de compartiment spécifiques à des fins de vérification de la disponibilité ou de la sécurité. Pour obtenir des instructions sur l'attribution des noms, consultez Règles de dénomination des compartiments à usage général.

Amazon S3 crée des compartiments dans une région que vous spécifiez. Pour réduire la latence, minimiser les coûts ou répondre aux exigences réglementaires, choisissez Région AWS celui qui est géographiquement proche de vous. Par exemple, si vous résidez en Europe, il peut être avantageux de créer des compartiments dans les régions Europe (Irlande) ou Europe (Francfort). Pour obtenir la liste des régions Amazon S3, consultez Régions et points de terminaison dans les Références générales AWS .

> **Note**
>
> Les objets appartenant à un compartiment que vous créez dans une région spécifique Région AWS ne quittent jamais cette région, sauf si vous les transférez explicitement vers une autre région. Par exemple, les objets stockés dans la région Europe (Irlande) ne la quittent jamais.

Modèles de seaux à usage général courants

Lorsque vous créez des applications sur Amazon S3, vous pouvez utiliser des compartiments uniques à usage général pour séparer les différents jeux de données ou les différentes charges de travail. En fonction de votre cas d'utilisation, il existe différents modèles de conception et les meilleures pratiques pour l'utilisation de seaux à usage général. Pour de plus amples informations, veuillez consulter Modèles de compartiments à usage général courants pour créer des applications sur Amazon S3.

Autorisations

Vous pouvez utiliser vos Utilisateur racine d'un compte AWS informations d'identification pour créer un compartiment à usage général et effectuer toute autre opération Amazon S3. Toutefois, nous vous recommandons de ne pas utiliser les informations d'identification d'utilisateur racine de votre Compte AWS pour effectuer des demandes, par exemple pour créer un compartiment. Il est préférable de créer un utilisateur AWS Identity and Access Management (IAM), puis de lui accorder un accès total (par défaut, les utilisateurs ne bénéficient d'aucune autorisation).

Ces utilisateurs sont appelés administrateurs. Vous pouvez utiliser les informations d'identification de l'utilisateur administrateur, au lieu des informations d'identification de l'utilisateur root de votre

compte, pour interagir avec AWS et effectuer des tâches, telles que créer un bucket, créer des utilisateurs et leur accorder des autorisations.

Pour plus d'informations, consultez Informations d'identification de l'Utilisateur racine d'un compte AWS et informations d'identification d'un utilisateur IAM dans Références générales AWS , ainsi que Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Celui Compte AWS qui crée une ressource possède cette ressource. Par exemple, si vous créez un utilisateur IAM dans votre compartiment Compte AWS et que vous lui accordez l'autorisation de créer un compartiment, l'utilisateur peut créer un compartiment. Cependant, le Compte AWS auquel est associé l'utilisateur est le propriétaire du compartiment, et non l'utilisateur. Pour que l'utilisateur puisse effectuer d'autres opérations sur les compartiments, le propriétaire de la ressource doit lui accorder d'autres autorisations. Pour plus d'informations sur la gestion des autorisations relatives à vos ressources Amazon S3, consultez Gestion des identités et des accès pour Amazon S3.

Gestion de l'accès du public aux compartiments à usage général

L'accès public est accordé aux compartiments et aux objets à usage général par le biais de politiques relatives aux compartiments, de listes de contrôle d'accès (ACLs) ou des deux. Pour vous aider à gérer l'accès public aux ressources Amazon S3, Amazon S3 fournit des paramètres permettant de bloquer l'accès public. Les paramètres d'accès public par blocage d'Amazon S3 peuvent remplacer ACLs les politiques relatives aux compartiments afin que vous puissiez appliquer des limites uniformes à l'accès public à ces ressources. Vous pouvez appliquer des paramètres de blocage de l'accès public à des compartiments individuels ou à tous les compartiments de votre compte.

Pour garantir que l'accès public de tous vos compartiments et objets Amazon S3 à usage général est bloqué, les quatre paramètres de blocage de l'accès public sont activés par défaut lorsque vous créez un nouveau compartiment. Nous vous recommandons d'activer ces quatre paramètres également pour votre compte. Ces paramètres bloquent tout accès public pour tous les compartiments présents et futurs.

Avant d'appliquer ces paramètres, vérifiez que vos applications fonctionnent correctement sans accès public. Si vous avez besoin d'un certain niveau d'accès public à vos compartiments ou objets (par exemple pour héberger un site Web statique, comme décrit dans Hébergement d'un site Web statique à l'aide d'Amazon S3), vous pouvez personnaliser les paramètres individuels afin de les adapter à vos cas d'utilisation du stockage. Pour plus d'informations, consultez Blocage de l'accès public à votre stockage Amazon S3.

Toutefois, nous vous recommandons vivement de garder l'option Bloquer l'accès public activée. Si vous souhaitez conserver les quatre paramètres de blocage de l'accès public activés et héberger un site Web statique, vous pouvez utiliser le contrôle CloudFront d'accès d'origine (OAC) d'Amazon. Amazon CloudFront fournit les fonctionnalités requises pour configurer un site Web statique sécurisé. Les sites Web statiques Amazon S3 prennent uniquement en charge les points de terminaison HTTP. Amazon CloudFront utilise le stockage durable d'Amazon S3 tout en fournissant des en-têtes de sécurité supplémentaires, tels que HTTPS. HTTPS accroît la sécurité en chiffrant une demande HTTP normale et en offrant une protection contre les cyberattaques courantes.

Pour plus d'informations, consultez Getting started with a secure static website in the Amazon CloudFront Developer Guide.

> **Note**
>
> Si un message indiquant `Error` quand vous listez vos compartiments à usage général et leurs paramètres d'accès public s'affiche, il se peut que vous ne disposiez pas des autorisations requises. Assurez-vous d'avoir ajouté les autorisations suivantes à votre politique utilisateur ou à votre politique de rôle :
>
> ```
> s3:GetAccountPublicAccessBlock
> s3:GetBucketPublicAccessBlock
> s3:GetBucketPolicyStatus
> s3:GetBucketLocation
> s3:GetBucketAcl
> s3:ListAccessPoints
> s3:ListAllMyBuckets
> ```
>
> Dans de rares cas, les demandes peuvent également échouer en raison d'une défaillance de la Région AWS .

Options de configuration des buckets à usage général

Amazon S3 propose différentes options vous permettant de configurer votre compartiment à usage général. Par exemple, vous pouvez configurer votre compartiment pour l'hébergement d'un site Web, le configurer afin qu'il enregistre tous les accès au compartiment, ou encore ajouter une configuration pour la gestion du cycle de vie des objets qu'il contient. Amazon S3 prend en charge des sous-ressources qui vous permettent de stocker et de gérer les informations relatives à la configuration

du compartiment. Vous pouvez utiliser l'API Amazon S3 pour créer et gérer ces sous-ressources. Toutefois, vous pouvez également utiliser la console ou le AWS SDKs.

> **Note**
>
> Les configurations au niveau de l'objet sont également possibles. Par exemple, vous pouvez configurer une liste de contrôle d'accès (ACL) spécifique à un objet, ce qui vous permet de configurer des autorisations au niveau de cet objet.

Nous parlons de « sous-ressources », car celles-ci se trouvent dans le contexte d'un compartiment ou d'un objet donnés. Le tableau ci-dessous répertorie les sous-ressources qui vous permettent de gérer les configurations associées à un compartiment donné.

Sous-ressource	Description
cors (partage des ressources cross-origin)	Vous pouvez configurer le compartiment afin d'autoriser les demandes cross-origin. Pour plus d'informations, consultez Utilisation du partage des ressources entre origines multiples (CORS).
event notification	Vous pouvez autoriser le compartiment à vous envoyer des notifications lorsque certains événements s'y produisent. Pour plus d'informations, consultez Notifications d'événements Amazon S3.
lifecycle	Vous pouvez définir des règles de cycle de vie pour des objets de votre compartiment, lorsque ceux-ci disposent d'un cycle de vie bien défini. Par exemple, vous pouvez définir une règle qui permet d'archiver certains objets un an après leur création ou de les supprimer 10 ans après leur création. Pour plus d'informations, consultez Gestion du cycle de vie des objets.
location	Lorsque vous créez un compartiment, vous spécifiez l' Région AWS endroit où vous souhaitez qu'Amazon S3 le crée. Amazon S3 stocke cette informati on dans la sous-ressource associée à l'emplacement et fournit une API qui vous permet de récupérer cette information.

Sous-ressource	Description
journalisation	La journalisation vous permet d'effectuer le suivi des demandes d'accès au compartiment. Chaque enregistrement de journal d'accès fournit des informations détaillées sur une demande d'accès donnée (demandeur, nom du compartiment, heure de la demande, action associée à la demande, état de la réponse et code d'erreur, le cas échéant). Les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Cela peut également vous aider à en savoir plus sur votre base de clients et à comprendre votre facture Amazon S3. Pour plus d'informations, consultez Enregistrement de demandes avec journalisation des accès au serveur.
Verrouillage d'objet	Pour utiliser le verrouillage des objets S3, vous devez l'activer pour un compartiment. Si vous le souhaitez, vous pouvez également configurer un mode et une période de rétention par défaut qui s'appliqueront aux nouveaux objets mis en place dans le compartiment. Pour plus d'informations, consultez Verrouillage d'objets avec la fonctionn alité de verrouillage d'objet.
policy et ACL (liste de contrôle d'accès)	Par défaut, toutes vos ressources (telles que les objets et compartim ents) sont privées. Amazon S3 prend en charge les options de liste de contrôle d'accès (ACL) et de politique de compartiment, qui vous permettent d'accorder et de gérer des autorisations au niveau du compartiment. Amazon S3 stocke les informations relatives aux autorisations dans les sous-ress ources policy et acl. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon S3.
réplication	La réplication est la copie automatique et asynchrone d'objets entre des compartiments dans des Régions AWS différents ou identiques. Pour de plus amples informations, veuillez consulter Réplication d'objets au sein des régions et entre elles.

Sous-ressource	Description
requestPayment	Par défaut, Compte AWS celui qui crée le bucket (le propriétaire du bucket) paie les téléchargements depuis le bucket. Toutefois, cette sous-ressource permet au propriétaire du compartiment de spécifier que l'utilisateur qui demande un téléchargement soit facturé lorsqu'il effectue un téléchargement. Amazon S3 fournit une API qui vous permet de gérer cette sous-ressource. Pour plus d'informations, consultez Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation.
tagging	Vous pouvez ajouter des balises de répartition des coûts à votre compartiment pour classer et suivre vos AWS coûts. Amazon S3 fournit la sous-ressource tagging qui vous permet de stocker et de gérer des balises sur un compartiment. A partir des balises intégrées à votre compartiment, AWS génère un rapport de répartition des coûts faisant apparaître la consommation et les coûts regroupés par les balises. Pour plus d'informations, consultez Rapports d'utilisation et de facturation pour Amazon S3.
Transfer Acceleration	Transfer Acceleration permet un transfert rapide, facile et sécurisé de fichiers à grande distance entre votre client et un compartiment S3. Transfer Acceleration tire parti des emplacements périphériques distribués dans le monde entier d'Amazon CloudFront. Pour de plus amples informations, veuillez consulter Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.
gestion des versions	La gestion des versions vous permet de récupérer un objet remplacé ou supprimé par erreur. La gestion des versions est une bonne pratique que nous recommandons pour la récupération d'objets remplacés ou supprimés par erreur. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Sous-ressource	Description
website	Vous pouvez configurer votre compartiment pour l'hébergement de sites Web statiques. Amazon S3 crée une sous-ressource website afin de stocker cette configuration. Pour de plus amples informations, veuillez consulter Hébergement d'un site Web statique à l'aide d'Amazon S3.

Fonctionnement des godets à usage général

L'ingénierie haute disponibilité d'Amazon S3 met l'accent sur les opérations get, put, list et delete. Étant donné que les opérations de bucket à usage général vont à l'encontre d'un espace de ressources global centralisé, nous vous recommandons de ne pas créer, supprimer ou configurer de compartiments sur le chemin du code de haute disponibilité de votre application. Il est préférable de les créer, de les supprimer ou de les configurer dans le cadre d'une routine d'initialisation ou de configuration distincte, que vous exécutez moins souvent.

Surveillance des performances des godets à usage général

Lorsque vos applications et processus métier critiques dépendent des AWS ressources, il est important de surveiller votre système et de recevoir des alertes pour celui-ci. La surveillance de vos données peut contribuer à préserver la fiabilité, la disponibilité et les performances d'Amazon S3 et de vos AWS solutions. Il existe plusieurs AWS services que vous pouvez utiliser pour collecter et agréger des métriques et des journaux pour vos compartiments S3.

En fonction de votre cas d'utilisation, vous pouvez choisir le AWS service le mieux adapté aux besoins de votre entreprise pour résoudre les problèmes, surveiller vos données, optimiser les coûts de stockage ou résoudre les problèmes multipoints. Par exemple :

- Pour améliorer les performances des applications qui utilisent S3 : configurez des CloudWatch alarmes pour surveiller vos données de stockage, vos métriques de réplication ou vos métriques de demande.
- Pour planifier l'utilisation du stockage, optimiser les coûts de stockage ou pour connaître la quantité de stockage dont vous disposez dans l'ensemble de votre organisation : utilisez Amazon S3 Storage Lens. Vous pouvez également utiliser S3 Storage Lens pour améliorer les performances

de vos données en activant des métriques avancées et en utilisant les métriques de code d'état détaillées pour obtenir le nombre de demandes réussies ou échouées.

- Pour une vue unifiée de l'état de vos opérations : publiez les indicateurs d'utilisation et d'activité de S3 Storage Lens sur un Amazon CloudWatch tableau de bord.

> **Note**
>
> L'option de Amazon CloudWatch publication est disponible pour les tableaux de bord S3 Storage Lens mis à niveau vers les métriques et recommandations avancées. Vous pouvez activer l'option de CloudWatch publication pour une configuration de tableau de bord nouvelle ou existante dans S3 Storage Lens.

- Pour obtenir un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service : configurez AWS CloudTrail des journaux. Vous pouvez également utiliser AWS CloudTrail les journaux pour examiner les appels d'API pour Amazon S3 sous forme d'événements.
- Pour recevoir des notifications concernant le moment où un certain événement se produit dans votre compartiment S3 : configurez les notifications d'événements Amazon S3.
- Pour obtenir des enregistrements détaillés des demandes adressées à un compartiment S3 : configurez les journaux d'accès S3.

Pour obtenir la liste des différents AWS services que vous pouvez utiliser pour surveiller vos données, consultez la section Journalisation et surveillance dans Amazon S3.

Modèles de compartiments à usage général courants pour créer des applications sur Amazon S3

Lorsque vous créez des applications sur Amazon S3, vous pouvez utiliser des compartiments uniques à usage général pour séparer les différents jeux de données ou les différentes charges de travail. Lorsque vous créez des applications destinées à des utilisateurs finaux ou à différents groupes d'utilisateurs, utilisez nos modèles de conception basés sur les bonnes pratiques pour créer des applications qui tirent le meilleur parti des fonctionnalités et de la capacité de mise à l'échelle d'Amazon S3.

> **Important**
>
> Nous vous recommandons de créer des noms de compartiments à usage général qui ne sont pas prévisibles. N'écrivez pas le code en présumant que le nom de compartiment que vous avez choisi est disponible, à moins que vous n'ayez déjà créé ce compartiment. Une méthode permettant de créer des noms de compartiment qui ne sont pas prévisibles consiste à ajouter un identifiant unique global (GUID) au nom du compartiment (`amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`, par exemple). Pour plus d'informations sur les règles de dénomination des compartiments à usage général, consultez Règles de dénomination des compartiments à usage général.

Rubriques

- Modèle de compartiment à usage général pour plusieurs locataires
- Bucket-per-use motif

Modèle de compartiment à usage général pour plusieurs locataires

Avec les compartiments à locataires multiples, vous créez un compartiment unique à usage général pour une équipe ou une charge de travail. Vous utilisez des préfixes S3 uniques pour organiser les objets que vous stockez dans ce compartiment. Un préfixe est une chaîne de caractères au début du nom de la clé d'objet. Il n'a pas de limite de longueur, mais ne peut pas dépasser la longueur du nom de la clé d'objet (1 024 octets). Vous pouvez voir les préfixes comme un moyen d'organiser vos données de la même manière que les répertoires. Toutefois, les préfixes ne sont pas des répertoires.

Par exemple, pour stocker des informations sur des villes, vous pouvez les organiser par continent, puis par pays, puis par province, région ou État. Étant donné que ces noms ne contiennent généralement pas de ponctuation, vous devez utiliser une barre oblique (/) comme délimiteur. Les exemples suivants présentent les préfixes utilisés pour organiser des noms de villes par continent, par pays, puis par province, région ou État à l'aide d'une barre oblique (/).

- Europe/France/NouvelleA-Aquitaine/Bordeaux
- Nord America/Canada/Quebec/Montreal
- Nord America/USA/Washington/Bellevue
- Nord America/USA/Washington/Seattle

Ce modèle s'adapte bien lorsque vous avez des centaines d'ensembles de données uniques dans un bucket à usage général. Grâce aux préfixes, vous pouvez facilement organiser et regrouper ces jeux de données.

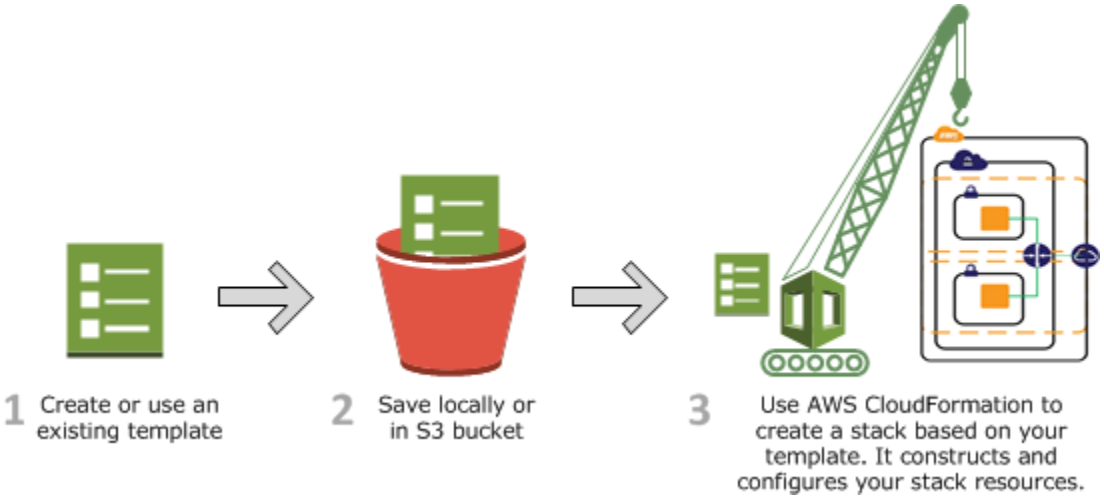
Cependant, l'un des inconvénients potentiels du modèle de bucket multi-tenant à usage général est que de nombreuses fonctionnalités au niveau du bucket S3, telles que le chiffrement des compartiments par défaut, le versionnement S3 et S3Requester Pays, sont définies au niveau du bucket et non au niveau du préfixe. Si les différents jeux de données du compartiment à locataires multiples ont des exigences uniques, il pourra être difficile de spécifier les paramètres corrects de chaque jeu de données, car vous ne pouvez pas configurer de nombreuses fonctionnalités au niveau du compartiment S3 au niveau du préfixe. En outre, dans un compartiment à locataires multiples, la répartition des coûts peut se compliquer à mesure que vous essayez de comprendre le stockage, les demandes et le transfert de données associés à des préfixes spécifiques.

Bucket-per-use motif

Avec le bucket-per-use modèle, vous créez un bucket à usage général pour chaque ensemble de données, utilisateur final ou équipe distinct. Comme vous pouvez configurer les fonctionnalités au niveau du compartiment S3 pour chacun de ces compartiments, vous pouvez utiliser ce modèle pour configurer des paramètres uniques au niveau du compartiment. Par exemple, vous pouvez configurer des fonctionnalités telles que le chiffrement des compartiments par défaut, la gestion des versions S3 et les paiements S3 par le demandeur de manière personnalisée en fonction du jeu de données de chaque compartiment. L'utilisation d'un compartiment pour chaque jeu de données, utilisateur final ou équipe distinct peut également vous aider à simplifier à la fois vos stratégies de gestion des accès et de répartition des coûts.

L'inconvénient potentiel de cette approche est que vous devrez gérer des milliers de compartiments. Tous Comptes AWS ont un quota par défaut de 10 000 compartiments à usage général. Pour augmenter le quota de compartiments d'un compte, vous pouvez soumettre une demande d'augmentation de quota. Pour demander une augmentation du quota de compartiments à usage général, accédez à la console Service Quotas.

Pour gérer votre bucket-per-use modèle et simplifier la gestion de votre infrastructure, vous pouvez utiliser AWS CloudFormation. Vous pouvez créer un AWS CloudFormation modèle personnalisé pour votre modèle qui définit déjà tous les paramètres souhaités pour vos compartiments S3 à usage général, afin de pouvoir facilement déployer et suivre les modifications apportées à votre infrastructure. Pour plus d'informations, consultez AWS::S3::Bucket dans le Guide de l'utilisateur AWS CloudFormation .



Règles de dénomination des compartiments à usage général

Lorsque vous créez un bucket à usage général, assurez-vous de prendre en compte la longueur, les caractères valides, le formatage et le caractère unique des noms de bucket. Les sections suivantes fournissent des informations sur la dénomination des compartiments à usage général, notamment les règles de dénomination, les bonnes pratiques et un exemple de création d'un compartiment à usage général avec un nom incluant un identifiant unique global (GUID).

Pour plus d'informations sur les noms de clés d'objets, consultez la section Création de noms de clés d'objets.

Pour créer un bucket à usage général, voirthe section called "Création d'un bucket à usage général".

Rubriques

- Règles de dénomination des compartiments à usage général
- Exemples de noms de compartiments à usage général
- Bonnes pratiques
- Création d'un compartiment qui utilise un GUID dans son nom

Règles de dénomination des compartiments à usage général

Les règles de dénomination suivantes s'appliquent aux compartiments à usage général.

- Les noms de compartiment peuvent comporter entre 3 (min.) et 63 (max.) caractères.

- Les noms de compartiments ne peuvent être composés que de lettres minuscules, de chiffres, de points (`.`) et de tirets (). -
- Les noms de compartiment doivent commencer et se terminer par une lettre ou un chiffre.
- Les noms de compartiment ne doivent pas contenir deux points consécutifs.
- Les noms des compartiments ne doivent pas être formatés en tant qu'adresse IP (par exemple,`192.168.5.4`).
- Les noms de compartiment ne doivent pas commencer par le préfixe `xn--`.
- Les noms de compartiment ne doivent pas commencer par le préfixe `sthree-`.
- Les noms de compartiment ne doivent pas commencer par le préfixe `amzn-s3-demo-`.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `-s3alias`. Ce suffixe est réservé aux noms d'alias de point d'accès. Pour plus d'informations, consultez Alias de point d'accès.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `--ol-s3`. Ce suffixe est réservé aux noms d'alias de point d'accès Object Lambda. Pour de plus amples informations, veuillez consulter Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda de compartiment S3.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `.mrap`. Ce suffixe est réservé aux noms de point d'accès multi-régions. Pour de plus amples informations, veuillez consulter Règles relatives à l'attribution de noms pour les points d'accès multi-Régions Amazon S3.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `--x-s3`. Ce suffixe est réservé aux compartiments de répertoires. Pour de plus amples informations, veuillez consulter Règles de dénomination des compartiments de répertoires.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `--table-s3`. Ce suffixe est réservé aux buckets S3 Tables. Pour de plus amples informations, veuillez consulter Règles de dénomination des compartiments de tables, des tables et des espaces de noms Amazon S3.
- Les buckets utilisés avec Amazon S3 Transfer Acceleration ne peuvent pas avoir de points (`.`) dans leur nom. Pour plus d'informations sur Transfer Acceleration, consultez Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.

> **Important**
>
> - Les noms des compartiments doivent être uniques Comptes AWS dans tous les compartiments Régions AWS d'une partition. Une partition est un regroupement de

régions. AWS possède actuellement trois partitions : `aws` (Régions commerciales), `aws-cn` (Régions de Chine) et `aws-us-gov` (AWS GovCloud (US) Régions).

- Le nom d'un bucket ne peut pas être utilisé par un autre Compte AWS utilisateur de la même partition tant que le bucket n'est pas supprimé. Après avoir supprimé un bucket, sachez qu'un autre Compte AWS de la même partition peut utiliser le même nom de bucket pour un nouveau bucket et peut donc potentiellement recevoir des demandes destinées au bucket supprimé. Si vous souhaitez empêcher cela, ou si vous souhaitez continuer à utiliser le même nom de bucket, ne supprimez pas le bucket. Nous vous recommandons de vider le compartiment et de le conserver, et de bloquer toutes les demandes de compartiment selon les besoins. Pour les seaux qui ne sont plus utilisés activement, nous recommandons de vider le seau de tous les objets afin de minimiser les coûts tout en conservant le seau lui-même.
- Lorsque vous créez un bucket à usage général, vous choisissez son nom et le nom dans lequel le Région AWS créer. Une fois le compartiment à usage général créé, vous ne pouvez plus changer son nom ni sa région.
- N'incluez pas d'informations sensibles dans le nom du bucket. Le nom du bucket est visible URLs là où pointent les objets du bucket.

> **Note**
>
> Avant le 1er mars 2018, les compartiments créés dans la région USA Est (Virginie du Nord) pouvaient comporter des noms incluant jusqu'à 255 caractères et comprenant des lettres majuscules et des traits de soulignement. À compter du 1er mars 2018, les nouveaux compartiments de la région USA Est (Virginie du Nord) doivent être conformes aux règles appliquées dans toutes les autres régions.

Exemples de noms de compartiments à usage général

Les noms de compartiment suivants présentent des exemples de caractères autorisés dans les noms de compartiments à usage général : a-z, 0-9 et tirets (). `-` Le préfixe `amzn-s3-demo-` réservé n'est utilisé ici qu'à titre d'illustration. Comme il s'agit d'un préfixe réservé, vous ne pouvez pas créer de noms de bucket commençant par. `amzn-s3-demo-`

- `amzn-s3-demo-bucket1-a1b2c3d4-5678-90ab-cdef-example11111`

- `amzn-s3-demo-bucket`

Les exemples de noms de bucket suivants sont valides mais déconseillés pour des utilisations autres que l'hébergement statique de sites Web, car ils contiennent des points (`.`) :

- `example.com`
- `www.example.com`
- `my.example.s3.bucket`

Les exemples de noms de compartiment suivants ne sont pas valides :

- `amzn_s3_demo_bucket` (contient des traits de soulignement)
- `AmznS3DemoBucket` (contient des lettres majuscules)
- `amzn-s3-demo-bucket-`(commence par un `amzn-s3-demo-` préfixe et se termine par un trait d'union)
- `example..com`(contient deux points d'affilée)
- `192.168.5.4`(correspond au format d'une adresse IP)

Bonnes pratiques

Lorsque vous nommez vos compartiments à usage général, tenez compte des meilleures pratiques suivantes en matière de dénomination des compartiments.

Choisissez un schéma de dénomination des compartiments peu susceptible de provoquer des conflits de dénomination

Si votre application crée automatiquement des compartiments, choisissez un schéma de dénomination des compartiments peu susceptible de provoquer des conflits de dénomination. Vous devez veiller à ce que la logique applicative sélectionne un autre nom lorsqu'un nom de compartiment est déjà utilisé.

Ajouter des identificateurs uniques globaux (GUIDs) aux noms de compartiments

Nous vous recommandons de créer des noms de compartiments imprévisibles. N'écrivez pas de code en supposant que le nom de compartiment que vous avez choisi est disponible, sauf si vous l'avez déjà créé. Une méthode pour créer des noms de compartiment imprévisibles consiste à ajouter

un identifiant global unique (GUID) au nom de votre compartiment, par exemple,. `amzn-s3-demo-bucket-a1b2c3d4-5678-90ab-cdef-example11111` Pour de plus amples informations, veuillez consulter the section called "Création d'un compartiment qui utilise un GUID dans son nom".

Évitez d'utiliser des points (`.`) dans les noms de compartiments

Pour une compatibilité optimale, nous vous recommandons d'éviter d'utiliser des points (`.`) dans les noms de bucket, sauf pour les buckets utilisés uniquement pour l'hébergement de sites Web statiques. Si vous incluez des points dans le nom d'un bucket, vous ne pouvez pas utiliser l' virtual-host-styleadressage via HTTPS, sauf si vous validez vous-même le certificat. Les certificats de sécurité utilisés pour l'hébergement virtuel des buckets ne fonctionnent pas pour les buckets dont le nom contient des points.

Cette limitation n'affecte pas les compartiments utilisés pour l'hébergement de sites Web statiques, car l'hébergement de sites Web statiques n'est disponible que via HTTP. Pour plus d'informations sur l' virtual-host-styleadressage, consultezHébergement virtuel de buckets à usage général. Pour plus d'informations sur l'hébergement de sites web statiques, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.

Choisir un nom pertinent

Lorsque vous nommez un bucket, nous vous recommandons de choisir un nom pertinent pour vous ou pour votre entreprise. Évitez d'utiliser des noms associés à d'autres. Par exemple, évitez d'utiliser `AWS` ou `Amazon` dans le nom de votre compartiment.

Ne supprimez pas de compartiments afin de pouvoir réutiliser les noms des compartiments

Si un compartiment est vide, vous pouvez le supprimer. Une fois qu'un compartiment a été supprimé, son nom peut être réutilisé. Cependant, il n'est pas garanti que vous puissiez réutiliser le nom immédiatement, ou pas du tout. Après avoir supprimé un bucket, il peut s'écouler un certain temps avant que vous puissiez réutiliser le nom. En outre, un autre Compte AWS utilisateur peut créer un bucket portant le même nom avant que vous puissiez le réutiliser.

Après avoir supprimé un compartiment à usage général, sachez qu'un autre Compte AWS compartiment de la même partition peut utiliser le même nom de compartiment pour un nouveau compartiment et peut donc potentiellement recevoir des demandes destinées au compartiment à usage général supprimé. Si vous souhaitez empêcher cela, ou si vous souhaitez continuer à utiliser le même nom de bucket à usage général, ne supprimez pas le bucket à usage général. Nous vous recommandons de vider le compartiment et de le conserver, et de bloquer toutes les demandes de compartiment selon les besoins.

Création d'un compartiment qui utilise un GUID dans son nom

Les exemples suivants vous montrent comment créer un compartiment à usage général incluant un GUID à la fin de son nom.

À l'aide du AWS CLI

L' AWS CLI exemple suivant crée un bucket à usage général dans la région USA Ouest (Californie du Nordus-west-1) () avec un exemple de nom de bucket utilisant un identifiant global unique (GUID). Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

Utilisation du AWS SDK pour Java

L'exemple suivant vous montre comment créer un avec un GUID à la fin du nom du compartiment dans la région USA Est (Virginie du Nord) (us-east-1) en utilisant le AWS SDK pour Java. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations. Pour plus d'informations sur les autres AWS SDKs, voir Outils sur lesquels s'appuyer AWS.

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
```

```
        s3.createBucket(createRequest);
    }
}
```

Quotas, limites et restrictions relatifs aux compartiments à usage général

Un bucket Amazon S3 à usage général appartient à Compte AWS celui qui l'a créé. La propriété du compartiment n'est pas transférable à un autre compte.

Quotas de compartiments

Par défaut, vous pouvez créer jusqu'à 10 000 compartiments à usage général par. Compte AWS Pour demander une augmentation du quota de compartiments à usage général, accédez à la console Service Quotas.

> **Important**
>
> Nous vous recommandons vivement de n'utiliser que des demandes `ListBuckets` paginées. Les demandes `ListBuckets` non paginées ne sont prises en charge que pour les Comptes AWS dont le quota de compartiments à usage général par défaut a été défini sur 10 000. Si vous avez un quota de compartiments à usage général approuvé supérieur à 10 000, vous devez envoyer des demandes `ListBuckets` paginées pour répertorier les compartiments de votre compte. Toutes les `ListBuckets` demandes non paginées seront rejetées si le quota de Comptes AWS compartiments à usage général est supérieur à 10 000.

> **Note**
>
> Vous devez utiliser les informations suivantes Régions AWS pour consulter votre quota, l'utilisation des compartiments ou demander une augmentation de vos compartiments à usage général dans votre Compte AWS.
>
> - Les quotas de compartiments à usage général pour les régions commerciales ne peuvent être consultés et gérés qu'à partir de la région USA Est (Virginie du Nord).
> - Les quotas de bucket à usage général pour ne AWS GovCloud (US) peuvent être consultés et gérés qu'à partir de AWS GovCloud (US-West).

Pour plus d'informations sur les quotas de service, consultez Quotas de service AWS dans la Référence générale d'Amazon Web Services.

Limitations sur les objets et compartiments

Il n'y a pas de taille de compartiment maximale ou de limite au nombre d'objets que vous pouvez stocker dans un compartiment. Vous pouvez également choisir de stocker tous vos objets dans un seul compartiment ou les répartir dans différents compartiments. Toutefois, vous ne pouvez pas créer un compartiment au sein d'un autre compartiment.

Règles d'attribution de noms pour les compartiments

Lorsque vous créez un bucket, vous choisissez son nom et le Région AWS nom dans lequel le créer. Une fois le compartiment créé, vous ne pouvez pas changer son nom ni sa région. Pour plus d'informations sur l'attribution de noms à des compartiments, reportez-vous à la section Règles de dénomination des compartiments à usage général.

Accès à un compartiment à usage général Amazon S3

Vous pouvez accéder à vos compartiments à usage général Amazon S3 à l'aide de la console Amazon S3 ou de l'API REST Amazon S3. AWS Command Line Interface AWS SDKs Chaque méthode d'accès à un compartiment S3 à usage général prend en charge des cas d'utilisation spécifiques. Pour plus d'informations, consultez les sections suivantes.

Rubriques

- Cas d'utilisation
- Console Amazon S3
- AWS CLI
- AWS SDKs
- API REST Amazon S3

Cas d'utilisation

Selon le cas d'utilisation de votre compartiment à usage général Amazon S3, différentes méthodes sont recommandées pour accéder aux données sous-jacentes de vos compartiments. La liste suivante inclut les cas d'utilisation courants pour accéder à vos données.

- Sites web statiques : vous pouvez utiliser Amazon S3 pour héberger un site web statique. Dans ce cas d'utilisation, vous pouvez configurer votre bucket S3 à usage général pour qu'il fonctionne comme un site Web. Pour obtenir un exemple qui explique les différentes étapes d'hébergement d'un site web sur Amazon S3, consultez Didacticiel : configuration d'un site web statique sur Amazon S3.

  Pour héberger un site Web statique avec des paramètres de sécurité tels que le blocage de l'accès public activé, nous vous recommandons d'utiliser Amazon CloudFront avec Origin Access Control (OAC) et d'implémenter des en-têtes de sécurité supplémentaires, tels que HTTPS. Pour plus d'informations, consultez Démarrer avec un site web statique sécurisé.

  > **Note**
  >
  > Amazon S3 prend en charge à la fois le style d'hébergement virtuel et le style de chemin pour l'accès statique aux sites Web. URLs Étant donné que les buckets sont accessibles en utilisant le style de chemin et le style d'hébergement virtuel URLs, nous vous recommandons de créer des buckets avec des noms de bucket conformes au DNS. Pour de plus amples informations, veuillez consulter Quotas, limites et restrictions relatifs aux compartiments à usage général.

- Ensembles de données partagés : lorsque vous évoluez sur Amazon S3, il est courant d'adopter un modèle multi-tenant, dans lequel vous attribuez à différents clients finaux ou unités commerciales des préfixes uniques au sein d'un compartiment à usage général partagé. En utilisant les points d'accès Amazon S3, vous pouvez diviser une politique de compartiment de grande taille en politiques de point d'accès distinctes et discrètes pour chaque application devant accéder au jeu de données partagé. Cette approche permet de se concentrer plus simplement sur l'élaboration de la stratégie d'accès appropriée à une application sans perturber les activités des autres applications dans le jeu de données partagé. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .
- Charges de travail à haut débit — Mountpoint pour Amazon S3 est un client de fichiers open source à haut débit permettant de monter un bucket Amazon S3 à usage général en tant que système de fichiers local. Avec Mountpoint, vos applications peuvent accéder aux objets stockés dans Amazon S3 par le biais d'opérations de système de fichiers, telles qu'ouvrir et lire. Mountpoint traduit automatiquement ces opérations en appels d'API d'objet S3, permettant à vos applications d'accéder au stockage et au débit élastiques d'Amazon S3 via une interface de fichier. Pour de plus amples informations, veuillez consulter Monter un compartiment Amazon S3 en tant que système de fichiers local.

- Applications multirégionales : les points d'accès multirégionaux Amazon S3 fournissent un point de terminaison global que les applications peuvent utiliser pour répondre aux demandes provenant de compartiments S3 à usage général situés dans plusieurs compartiments. Régions AWS Vous pouvez utiliser des points d'accès multi-régions pour créer des applications multi-régions avec la même architecture utilisée dans une seule région, puis exécuter ces applications partout dans le monde. Au lieu d'envoyer les demandes sur l'Internet public, les points d'accès multi-régions offrent une résilience de réseau intégrée avec une accélération des demandes Internet vers Amazon S3. Pour de plus amples informations, veuillez consulter Gestion du trafic multirégional avec des points d'accès multirégionaux.
- Protocole de transfert de fichiers (SFTP) Secure Shell (SSH) : si vous essayez de transférer des données sensibles en toute sécurité sur Internet, vous pouvez utiliser un serveur compatible SFTP avec votre compartiment à usage général Amazon S3. AWS SFTP est un protocole réseau qui prend en charge toutes les fonctionnalités de sécurité et d'authentification du SSH. Avec ce protocole, vous avez un contrôle précis sur l'identité des utilisateurs, les autorisations et les clés ou vous pouvez utiliser des politiques IAM pour gérer l'accès. Pour associer un serveur compatible SFTP à votre compartiment Amazon S3, assurez-vous de créer votre serveur compatible SFTP en premier. Ensuite, vous configurez des comptes utilisateurs et associez le serveur à un compartiment Amazon S3 à usage général. Pour une présentation détaillée de ce processus, consultez AWS Transfer for SFTP — Service SFTP entièrement géré pour Amazon S3 dans AWS les blogs.

Console Amazon S3

La console est une interface utilisateur Web permettant de gérer Amazon S3 et ses AWS ressources. Avec la console Amazon S3, vous pouvez facilement accéder à un compartiment et modifier ses propriétés. Vous pouvez également effectuer la plupart des opérations sur les compartiments à l'aide de l'interface utilisateur de la console, sans écrire de code.

Si vous vous êtes inscrit à un Compte AWS, vous pouvez accéder à la console Amazon S3 en vous connectant à la console Amazon S3 et en choisissant S3 sur la page d'accueil de la console Amazon S3. Vous pouvez également utiliser ce lien pour accéder directement au https://console.aws.amazon.com/s3/.

AWS CLI

Vous pouvez utiliser le AWS CLI pour émettre des commandes ou créer des scripts sur la ligne de commande de votre système afin d'effectuer des tâches AWS (y compris S3). Par exemple, si vous

devez accéder à plusieurs compartiments, vous pouvez gagner du temps en automatisant AWS CLI les tâches courantes et répétitives. La scriptabilité et la reproductibilité des actions courantes sont fréquemment prises en compte à mesure que les entreprises évoluent.

AWS CLIFournit des commandes pour un large éventail de Services AWS. AWS CLI II est pris en charge sur Windows, macOS et Linux. Consultez le AWS Command Line Interface Guide de l'utilisateur pour démarrer. Pour plus d'informations sur les commandes d'Amazon S3, consultez les sections s3api et s3control dans la Référence des commandes de l'AWS CLI .

AWS SDKs

AWS fournit SDKs (kits de développement logiciel) composés de bibliothèques et d'exemples de code pour différents langages de programmation et plateformes (Java, Python, Ruby, .NET, iOS, Android, etc.). Ils AWS SDKs fournissent un moyen pratique de créer un accès programmatique à S3 et AWS. Amazon S3 est un service REST. Vous pouvez envoyer des demandes à Amazon S3 à l'aide des bibliothèques du AWS SDK, qui encapsulent l'API REST Amazon S3 sous-jacente et simplifient vos tâches de programmation. Par exemple, ils SDKs se chargent de tâches telles que le calcul des signatures, la signature cryptographique des demandes, la gestion des erreurs et le renouvellement automatique des demandes. Pour plus d'informations sur les AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils pour AWS.

Chaque interaction avec Amazon S3 est authentifiée ou anonyme. Si vous utilisez le AWS SDKs, les bibliothèques calculent la signature pour l'authentification à partir des clés que vous fournissez. Pour plus d'informations sur la façon d'adresser des demandes à Amazon S3, consultez Envoi de demandes.

API REST Amazon S3

L'architecture d'Amazon S3 a été conçue de manière à être neutre en termes de langage de programmation et utilise nos interfaces supportées par AWS pour stocker et récupérer des objets. Vous pouvez accéder à S3 et à AWS par programmation à l'aide de l'API REST Amazon S3. L'API REST est une interface HTTP pour Amazon S3. Lorsque vous utilisez l'API REST, vous utilisez des demandes HTTP standard pour créer, récupérer et supprimer des compartiments et des objets.

Pour utiliser l'API REST, vous pouvez choisir n'importe quelle boîte à outils prenant en charge HTTP. Vous pouvez même utiliser un explorateur pour récupérer des objets, si ceux-ci peuvent être lus de manière anonyme.

L'API REST utilise les codes de statut et en-têtes HTTP standard afin de permettre aux explorateurs et boîtes à outils classiques de fonctionner. Dans certains zones, nous avons ajouté des

fonctionnalités à HTTP (par exemple, nous avons ajouté des en-têtes afin de permettre le contrôle d'accès). Dans ces cas précis, nous avons fait notre possible pour intégrer cette nouvelle fonctionnalité de sorte qu'elle corresponde à la manière dont HTTP est généralement utilisé.

Si vous faites des appels directs d'API REST dans votre application, vous devez écrire le code pour calculer la signature et l'ajouter à la demande. Pour plus d'informations sur la façon d'adresser des demandes à Amazon S3, consultez Envoi de demandes dans la Référence d'API Amazon S3.

Hébergement virtuel de buckets à usage général

L'hébergement virtuel consiste à servir plusieurs sites web à partir d'un seul serveur web. Une façon de différencier les sites dans vos demandes d'API REST Amazon S3 consiste à utiliser le nom d'hôte apparent du Request-URI plutôt que simplement la partie du nom du chemin de l'URI. Une demande REST Amazon S3 ordinaire spécifie un compartiment en utilisant le premier composant délimité par une barre oblique du chemin de l'URI de demande. Vous pouvez plutôt utiliser l'hébergement virtuel Amazon S3 pour adresser un compartiment à usage général dans un appel d'API REST en utilisant l'`Host`en-tête HTTP. En pratique, Amazon S3 interprète `Host` en ce sens que la plupart des compartiments sont automatiquement accessibles (pour un type limité de demandes) à l'adresse `https://`*`bucket-name`*`.s3.`*`region-code`*`.amazonaws.com`. Pour obtenir la liste complète des régions et points de terminaison Amazon S3, consultez Points de terminaison et quotas Amazon S3 dans le Référence générale d'Amazon Web Services.

L'hébergement virtuel présente d'autres avantages. Par ailleurs, en nommant le compartiment après avoir enregistré le nom de domaine et en faisant de ce nom un alias DNS pour Amazon S3, vous pouvez totalement personnaliser l'URL des ressources Amazon S3, par exemple, `http://my.`*`bucket-name`*`.com/`. Vous pouvez également publier dans le « répertoire racine » du serveur virtuel de votre compartiment. Cet avantage peut être considérable car beaucoup d'applications existantes recherchent des fichiers dans cet emplacement standard. Par exemple, on peut s'attendre à ce que les fichiers `favicon.ico`, `robots.txt` et `crossdomain.xml` se trouvent tous à la racine.

> **Important**
>
> Lorsque vous utilisez des compartiments à usage général de type hébergé virtuellement avec SSL, le certificat SSL générique correspond uniquement aux compartiments ne contenant pas de points (). `.` Pour contourner cette limitation, utilisez HTTP ou écrivez votre propre logique de vérification de certificat. Pour plus d'informations, consultez Amazon S3 Path

Deprecation Plan (Plan d'obsolescence de chemin d'accès Amazon S3) sur la page AWS News Blog.

Rubriques

- Demandes de type chemin d'accès
- Demandes de type hébergement virtuel
- Spécification d'un compartiment d'en-tête Host HTTP
- Exemples
- Personnalisation d'Amazon S3 URLs avec des enregistrements CNAME
- Comment associer un nom d'hôte à un compartiment Amazon S3
- Limites
- Rétrocompatibilité

Demandes de type chemin d'accès

Amazon S3 prend actuellement en charge l'accès aux URL de type hébergement virtuel et chemin d'accès dans toutes les Régions AWS. Cependant, le style path-style URLs sera abandonné à l'avenir. Pour plus d'informations, consultez la remarque importante suivante.

Dans Amazon S3, le style de chemin URLs utilise le format suivant :

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

Par exemple, si vous créez un compartiment nommé `amzn-s3-demo-bucket1` dans la Région USA Ouest (Oregon) et que vous souhaitez accéder à l'objet `puppy.jpg` dans ce compartiment, vous pouvez utiliser l'URL de type chemin suivant :

```
https://s3.us-west-2.amazonaws.com/amzn-s3-demo-bucket1/puppy.jpg
```

Important

Mise à jour (23 septembre 2020) — Pour nous assurer que les clients disposent du temps nécessaire pour passer au style hébergé virtuel URLs, nous avons décidé de retarder la

dépréciation du style path. URLs Pour plus d'informations, consultez Amazon S3 Path Deprecation Plan – The Rest of the Story dans le blog dédié aux actualités d'AWS .

> **Warning**
>
> Lorsque vous hébergez du contenu de site Web qui sera accessible depuis un navigateur Web, évitez d'utiliser le style de chemin URLs, car cela pourrait interférer avec le modèle de sécurité d'origine identique au navigateur. Pour héberger le contenu d'un site Web, nous vous recommandons d'utiliser des points de terminaison du site Web S3 ou une CloudFront distribution. Pour plus d'informations, consultez Points de terminaison de sites web et Déployez une application monopage basée sur React sur Amazon S3 et CloudFront dans les modèles de guidage AWS Perspective.

Demandes de type hébergement virtuel

Dans un URI de type hébergement virtuel, le nom du compartiment fait partie du nom de domaine compris dans l'URL.

Le style Amazon S3 URLs virtual-hosted—utilise le format suivant :

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

Dans cet exemple, `amzn-s3-demo-bucket1` représente le nom de compartiment, USA Ouest (Oregon) représente la Région et `puppy.png` est le nom de la clé :

```
https://amzn-s3-demo-bucket1.s3.us-west-2.amazonaws.com/puppy.png
```

Spécification d'un compartiment d'en-tête **`Host`** HTTP

Tant que la demande `GET` n'utilise pas le point de terminaison SSL, vous pouvez spécifier le compartiment pour la demande grâce à l'en-tête `Host` HTTP. L'en-tête `Host` dans la demande REST est interprété comme suit :

- Si l'en-tête `Host` est omis ou que sa valeur est `s3.region-code.amazonaws.com`, le compartiment de la demande est le premier composant délimité par une barre oblique de l'URI de demande, et la clé de la demande constitue le reste de l'URI de demande. Il s'agit de la méthode

ordinaire, comme illustré par le premier et le deuxième exemples de cette section. L'omission de l'en-tête `Host` est valide uniquement pour les demandes HTTP 1.0.

- Sinon, si la valeur de l'en-tête `Host` se termine par `.s3.`*`region-code`*`.amazonaws.com`, le nom du compartiment est le composant de tête de la valeur de l'en-tête `Host` jusqu'à `.s3.`*`region-code`*`.amazonaws.com`. La clé de la demande est l'URI de demande. Cette interprétation expose les compartiments en tant que sous-domaines de `.s3.`*`region-code`*`.amazonaws.com`, comme illustré par les troisième et quatrième exemples de cette section.
- Sinon, le compartiment pour la demande est la valeur en minuscule de l'en-tête `Host`, et la clé pour la demande est l'URI de demande. Cette interprétation est utile lorsque vous avez enregistré le même nom DNS que votre nom de compartiment et que vous avez configuré ce nom comme alias de nom canonique (CNAME) pour Amazon S3. La procédure pour enregistrer des noms de domaine et configurer des enregistrements DNS CNAME n'entre pas dans le champ d'application de ce guide, mais le résultat est illustré par l'exemple final de cette section.

Exemples

Cette section fournit des exemples URLs et des demandes.

Example — Style de chemin et demandes URLs

Cet exemple utilise les éléments suivants :

- Nom de compartiment - `example.com`
- Région - USA Est (Virginie du Nord)
- Nom de clé - `homepage.html`

L'URL se présente comme suit :

```
http://s3.us-east-1.amazonaws.com/example.com/homepage.html
```

La demande se présente comme suit :

```
GET /example.com/homepage.html HTTP/1.1
Host: s3.us-east-1.amazonaws.com
```

La demande avec HTTP 1.0 et l'omission de l'en-tête `Host` se présentent comme suit :

```
GET /example.com/homepage.html HTTP/1.0
```

Pour en savoir plus sur les noms compatibles avec le DNS, consultez Limitations. Pour en savoir plus sur les clés, consultez Clés.

Example — Style et requêtes hébergés URLs virtuellement

Cet exemple utilise les éléments suivants :

- Nom de compartiment : `amzn-s3-demo-bucket1`
- Région : Europe (Irlande)
- Nom de clé : `homepage.html`

L'URL se présente comme suit :

```
http://amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com/homepage.html
```

La demande se présente comme suit :

```
GET /homepage.html HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.eu-west-1.amazonaws.com
```

Example – Méthode d'alias CNAME

Pour utiliser cette méthode, vous devez configurer votre nom DNS en tant qu'alias CNAME pour *`bucket-name`*`.s3.us-east-1.amazonaws.com`. Pour de plus amples informations, veuillez consulter Personnalisation d'Amazon S3 URLs avec des enregistrements CNAME.

Cet exemple utilise les éléments suivants :

- Nom de compartiment - `example.com`
- Nom de clé : `homepage.html`

L'URL se présente comme suit :

```
http://www.example.com/homepage.html
```

L'exemple se présente comme suit :

```
GET /homepage.html HTTP/1.1
Host: www.example.com
```

Personnalisation d'Amazon S3 URLs avec des enregistrements CNAME

Selon vos besoins, vous préférerez peut-être que `s3.region-code.amazonaws.com` n'apparaisse pas sur votre site web ou service. Par exemple, si vous hébergez des images de site web sur Amazon S3, vous pourriez préférer `http://images.example.com/` à `http://images.example.com.s3.us-east-1.amazonaws.com/`. Tout compartiment avec un nom compatible DNS peut être référencé comme suit : `http://BucketName.s3.Region.amazonaws.com/[Filename]`, par exemple, `http://images.example.com.s3.us-east-1.amazonaws.com/mydog.jpg`. Grâce au CNAME, vous pouvez mapper `images.example.com` à un nom d'hôte Amazon S3 pour que l'URL précédente puisse devenir `http://images.example.com/mydog.jpg`.

Votre nom de compartiment doit être identique à CNAME. Par exemple, si vous créez un CNAME pour mapper `images.example.com` à `images.example.com.s3.us-east-1.amazonaws.com`, `http://images.example.com/filename` et `http://images.example.com.s3.us-east-1.amazonaws.com/filename` seront identiques.

L'enregistrement du DNS CNAME doit donner au nom de domaine comme alias le nom d'hôte de type hébergement virtuel approprié. Par exemple, si le nom du compartiment et le nom de domaine sont `images.example.com` et que votre compartiment se trouve dans la Région USA Est (Virginie du Nord), l'enregistrement CNAME doit avoir comme alias `images.example.com.s3.us-east-1.amazonaws.com`.

```
images.example.com CNAME    images.example.com.s3.us-east-1.amazonaws.com.
```

Amazon S3 utilise le nom d'hôte pour déterminer le nom du compartiment. C'est pourquoi le CNAME et le nom du compartiment doivent être identiques. Par exemple, admettons que vous avez configuré `www.example.com` comme CNAME pour `www.example.com.s3.us-east-1.amazonaws.com`. Lorsque vous accédez à `http://www.example.com`, Amazon S3 reçoit une demande semblable à la suivante :

Example

```
GET / HTTP/1.1
Host: www.example.com
```

```
Date: date
Authorization: signatureValue
```

Amazon S3 voit uniquement le nom d'hôte d'origine `www.example.com` et n'a pas connaissance du mappage CNAME utilisé pour résoudre la demande.

Vous pouvez utiliser n'importe quel point de terminaison Amazon S3 dans un alias CNAME. Par exemple, `s3.ap-southeast-1.amazonaws.com` peut être utilisé dans les alias CNAME. Pour plus d'informations sur les points de terminaison, consultez la section Request endpoints dans le manuel Amazon S3 API Reference. Pour créer un site web statique à l'aide d'un domaine personnalisé, consultez Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53.

> **Important**
>
> Lorsque vous utilisez Custom URLs with CNAMEs, vous devez vous assurer qu'un bucket correspondant existe pour tout enregistrement CNAME ou alias que vous configurez. Par exemple, si vous créez des entrées DNS pour `www.example.com` et `login.example.com` afin de publier du contenu Web à l'aide de S3, vous devez créer les deux compartiments `www.example.com` et `login.example.com`.
>
> Lorsqu'un enregistrement CNAME ou un alias est configuré pour pointer vers un point de terminaison S3 sans compartiment correspondant, n'importe quel AWS utilisateur peut créer ce compartiment et publier du contenu sous l'alias configuré, même si le propriétaire n'est pas le même.
>
> Pour la même raison, nous vous recommandons de modifier ou de supprimer l'enregistrement CNAME ou d'alias correspondant lors de la suppression d'un compartiment.

Comment associer un nom d'hôte à un compartiment Amazon S3

Pour associer un nom d'hôte à un compartiment Amazon S3 à l'aide d'un alias CNAME

1. Sélectionnez un nom d'hôte qui appartient à un domaine que vous contrôlez.

   Cet exemple utilise le sous-domaine `images` du domaine `example.com`.
2. Créez un compartiment qui correspond au nom d'hôte.

   Dans cet exemple, les noms d'hôte et de compartiment sont `images.example.com`. Le nom du compartiment doit correspondre exactement au nom d'hôte.

3. Créez un enregistrement DNS CNAME qui définit le nom d'hôte comme alias du compartiment Amazon S3.

   Par exemple :

   ```
   images.example.com CNAME images.example.com.s3.us-west-2.amazonaws.com
   ```

   > **Important**
   >
   > Pour des raisons d'acheminement de demande, l'enregistrement DNS CNAME doit être défini exactement comme illustré dans l'exemple précédent. Sinon, il peut sembler fonctionner correctement, mais il entraînera à terme un comportement imprévisible.

   La procédure de configuration d'enregistrements DNS CNAME dépend de votre serveur ou fournisseur DNS. Pour obtenir des informations spécifiques, consultez la documentation du serveur ou contactez le fournisseur.

Limites

Les SOAP APIs pour Amazon S3 ne sont pas disponibles pour les nouveaux clients et approchent de leur fin de vie (EOL) le 31 août 2025. Nous vous recommandons d'utiliser l'API REST ou le AWS SDKs.

Rétrocompatibilité

Les sections suivantes couvrent divers aspects de la rétrocompatibilité Amazon S3 en ce qui concerne les demandes d'URL de type chemin d'accès et hébergement virtuel.

Points de terminaison hérités

Certaines Régions prennent en charge les points de terminaison hérités. Vous pouvez voir ces points de terminaison dans les journaux ou AWS CloudTrail journaux d'accès de votre serveur. Pour plus d'informations, consultez les informations suivantes. Pour obtenir la liste complète des régions et points de terminaison Amazon S3, consultez Points de terminaison et quotas Amazon S3 dans le Référence générale d'Amazon Web Services.

Important

Même si vous pouvez voir des points de terminaison hérités dans vos journaux, nous vous recommandons de toujours utiliser la syntaxe de point de terminaison standard pour accéder à vos compartiments.
Le style Amazon S3 URLs virtual-hosted—utilise le format suivant :

```
https://bucket-name.s3.region-code.amazonaws.com/key-name
```

Dans Amazon S3, le style de chemin URLs utilise le format suivant :

```
https://s3.region-code.amazonaws.com/bucket-name/key-name
```

S3-Région

Certaines régions Amazon S3 plus anciennes prennent en charge des points de terminaison contenant un tiret (`-`) entre `s3` et le code de région (par exemple, `s3-us-west-2`) au lieu d'un point (par exemple, `s3.us-west-2`). Si votre compartiment se trouve dans l'une de ces régions, le format de point de terminaison suivant peut s'afficher dans les journaux ou CloudTrail journaux d'accès au serveur :

```
https://bucket-name.s3-region-code.amazonaws.com
```

Dans cet exemple, le nom du bucket est amzn-s3-demo-bucket1 et la région est US West (Oregon) :

```
https://amzn-s3-demo-bucket1.s3-us-west-2.amazonaws.com
```

Point de terminaison global hérité

Pour certaines régions, vous pouvez utiliser le point de terminaison global hérité pour élaborer des demandes qui ne spécifient pas de point de terminaison spécifique à la région. Le point de terminaison global hérité est comme suit :

```
bucket-name.s3.amazonaws.com
```

Dans les journaux ou CloudTrail journaux d'accès de votre serveur, vous pouvez voir des demandes qui utilisent l'ancien point de terminaison global. Dans cet exemple, le nom du compartiment est `amzn-s3-demo-bucket1` et le point de terminaison global hérité est :

```
https://amzn-s3-demo-bucket1.s3.amazonaws.com
```

Demandes de type hébergement virtuel pour USA Est (Virginie du Nord)

Les demandes effectuées avec le point de terminaison global hérité sont transmises par défaut à la région USA Est (Virginie du Nord). Par conséquent, le point de terminaison global hérité est parfois utilisé à la place du point de terminaison Régional pour USA Est (Virginie du Nord). Si vous créez un compartiment dans la Région USA Est (Virginie du Nord) et que vous utilisez le point de terminaison global, Amazon S3 achemine votre demande vers cette Région par défaut.

Demandes de type hébergement virtuel pour d'autres régions

Le point de terminaison global hérité est également utilisé pour les demandes de type hébergement virtuel dans d'autres régions prises en charge. Si vous créez un compartiment dans une Région qui a été lancée avant le 20 mars 2019 et que vous utilisez le point de terminaison global hérité, Amazon S3 met à jour l'enregistrement DNS pour rediriger la demande vers l'emplacement correct, ce qui peut prendre du temps. Entre-temps, la règle par défaut s'applique et la demande de type hébergement virtuel est acheminée vers la région USA Est (Virginie du Nord). Amazon S3 la redirige ensuite avec une redirection temporaire HTTP 307 vers la région appropriée.

Pour les compartiments S3 situés dans des régions lancées après le 20 mars 2019, le serveur DNS n'achemine pas votre demande directement vers l' Région AWS endroit où réside votre compartiment. Au lieu de cela, il renvoie une erreur HTTP 400 Requête erronée. Pour plus d'informations, consultez Envoi de demandes dans la Référence d'API Amazon S3.

Demandes de type chemin d'accès

Pour la région USA Est (Virginie du Nord), vous pouvez utiliser le point de terminaison global hérité pour les demandes de type chemin d'accès.

Pour toutes les autres Régions, la syntaxe de type chemin exige l'utilisation du point de terminaison spécifique à la Région lors d'une tentative d'accès à un compartiment. Si vous essayez d'accéder à un bucket avec l'ancien point de terminaison global ou un autre point de terminaison différent de celui de la région où réside le bucket, vous recevez un code de réponse HTTP 301 Permanent Redirect error et un message indiquant l'URI correct pour votre ressource. Par exemple, si vous

utilisez `https://s3.amazonaws.com/bucket-name` un bucket créé dans la région de l'ouest des États-Unis (Oregon), vous recevrez une erreur de redirection permanente HTTP 301.

Création d'un bucket à usage général

Pour télécharger vos données sur Amazon S3, vous devez d'abord créer un compartiment Amazon S3 à usage général dans l'un des Régions AWS. Le Compte AWS qui crée le compartiment en est le propriétaire. Lorsque vous créez un compartiment, vous devez choisir un nom de compartiment et une Région. Au cours du processus de création, vous pouvez éventuellement choisir d'autres options de gestion du stockage pour le compartiment.

> **Important**
>
> Une fois que vous avez créé un bucket, vous ne pouvez pas modifier le nom du bucket, le propriétaire du bucket ou la région. Pour plus d'informations sur l'attribution de noms à des compartiments, reportez-vous à la section the section called "Règles de dénomination".

Par défaut, vous pouvez créer jusqu'à 10 000 compartiments à usage général par. Compte AWS Pour demander une augmentation du quota de compartiments à usage général, accédez à la console Service Quotas.

Chaque compartiment permet de stocker un nombre illimité d'objets. Pour obtenir la liste des restrictions et limitations relatives aux compartiments à usage général Amazon S3, consultezQuotas, limites et restrictions relatifs aux compartiments à usage général.

Réglages du godet à usage général

Lorsque vous créez un bucket à usage général, vous pouvez utiliser les paramètres suivants pour contrôler différents aspects du comportement de votre bucket :

- Propriété des objets S3 — La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour désactiver ou activer les listes de contrôle d'accès ()ACLs. Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsque cette option est ACLs désactivée, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

- Verrouillage des objets S3 — Le verrouillage des objets S3 peut aider à empêcher la suppression ou le remplacement des objets Amazon S3 pendant une durée déterminée ou indéfiniment. Object Lock utilise un modèle write-once-read-many(WORM) pour stocker des objets. Le verrouillage d'objet vous permet de satisfaire aux exigences réglementaires qui nécessitent le stockage WORM, ou bien d'ajouter une couche de protection supplémentaire contre la suppression et les modifications d'objets. Pour de plus amples informations, veuillez consulter the section called "Verrouillage d'objets ".

Après avoir créé un compartiment à usage général, ou lorsque vous créez un compartiment à usage général à l'aide de la console Amazon S3, vous pouvez également utiliser les paramètres suivants pour contrôler d'autres aspects du comportement de votre compartiment :

- Accès public aux blocs S3 : la fonctionnalité S3 Block Public Access fournit des paramètres pour les points d'accès, les compartiments et les comptes afin de vous aider à gérer l'accès public aux ressources Amazon S3. Par défaut, les nouveaux compartiments, points d'accès et objets n'autorisent pas l'accès public. Toutefois, les utilisateurs peuvent modifier les stratégies de compartiment, les stratégies de point d'accès ou les autorisations d'objet pour autoriser l'accès public. Les paramètres de la fonctionnalité de blocage de l'accès public S3 remplacent ces stratégies et autorisations pour que vous puissiez restreindre l'accès public à ces ressources. Pour de plus amples informations, veuillez consulter the section called "Blocage de l'accès public".
- Versionnage S3 : le versionnage est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment. La gestion des versions permet de récupérer facilement les données en cas d'actions involontaires des utilisateurs ou de défaillances des applications. Par défaut, le versionnement est désactivé pour les buckets. Pour de plus amples informations, veuillez consulter the section called "Conservation de plusieurs versions d'objets".
- Chiffrement par défaut : vous pouvez définir le type de chiffrement par défaut pour tous les objets de votre compartiment. Le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) est le niveau de base de la configuration du chiffrement pour chaque compartiment dans Amazon S3. Tous les nouveaux objets chargés dans un compartiment S3 sont automatiquement chiffrés avec SSE-S3 comme niveau de chiffrement de base. Si vous souhaitez utiliser un autre type de chiffrement par défaut, vous pouvez spécifier un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), un chiffrement double couche côté serveur avec des clés (DSSE-KMS) ou un chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C) pour chiffrer vos données. Pour de plus amples informations, veuillez consulter

Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.

Vous pouvez utiliser la console Amazon S3, l'API REST Amazon S3 AWS Command Line Interface (AWS CLI) ou AWS SDKs pour créer un bucket à usage général. Pour plus d'informations sur les autorisations requises pour créer un bucket à usage général, consultez le CreateBucketmanuel Amazon Simple Storage Service API Reference.

Si vous ne parvenez pas à créer un compartiment Amazon S3, consultez Comment résoudre les erreurs lors de la création d'un compartiment Amazon S3 ? sur AWS re:Post.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.

   > **Note**
   >
   > - Une fois le compartiment créé, vous ne pouvez pas changer sa région.
   > - Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste d'Amazon S3 Régions AWS, consultez la section sur les Service AWS points de terminaison dans le Référence générale d'Amazon Web Services.

3. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
4. Choisissez Créer un compartiment. La page Créer un compartiment s'ouvre.
5. Pour Nom du compartiment, saisissez le nom de votre compartiment.

   Le nom du compartiment doit présenter les caractéristiques suivantes :

   - Être unique dans une partition. Une partition est un regroupement de régions. AWS possède actuellement trois partitions : `aws` (Régions commerciales), `aws-cn` (Régions de Chine) et `aws-us-gov` (AWS GovCloud (US) Regions).
   - Il doit comporter entre 3 et 63 caractères.

- Composé uniquement de lettres minuscules, de chiffres, de points (.) et de traits d'union (). - Pour une compatibilité optimale, nous vous recommandons d'éviter d'utiliser des points (.) dans les noms de bucket, sauf pour les buckets utilisés uniquement pour l'hébergement de sites Web statiques.
- Il doit commencer et se terminer par une lettre ou un chiffre.
- Pour obtenir la liste complète des règles de dénomination des compartiments, consultez. Règles de dénomination des compartiments à usage général

> **Important**
>
> - Une fois le compartiment créé, vous ne pouvez pas changer son nom.
> - N'incluez pas d'informations sensibles dans le nom du bucket. Le nom du bucket est visible URLs là où pointent les objets du bucket.

6. (Facultatif) Sous Configuration générale, vous pouvez choisir de copier les paramètres d'un bucket existant dans votre nouveau bucket. Si vous ne souhaitez pas copier les paramètres d'un bucket existant, passez à l'étape suivante.

> **Note**
>
> Cette option :
>
> - N'est pas disponible dans la console Amazon S3 AWS CLI et n'est disponible que dans la console Amazon S3
> - Ne copie pas la politique du bucket du bucket existant vers le nouveau bucket

Pour copier les paramètres d'un compartiment existant, sous Copier les paramètres d'un compartiment existant, sélectionnez Choisir un compartiment. La fenêtre Choisir un compartiment s'ouvre. Recherchez le compartiment contenant les paramètres que vous souhaitez copier, puis sélectionnez Choisir un compartiment. La fenêtre Choisir un compartiment se ferme et la fenêtre Créer un compartiment s'ouvre à nouveau.

Sous Copier les paramètres d'un bucket existant, vous pouvez désormais voir le nom du bucket que vous avez sélectionné. Les paramètres de votre nouveau compartiment correspondent désormais aux paramètres du compartiment que vous avez sélectionné. Si vous souhaitez

supprimer les paramètres copiés, choisissez Restaurer les paramètres par défaut. Passez en revue les autres paramètres du bucket sur la page Créer un bucket. Si vous ne souhaitez apporter aucune modification, vous pouvez passer à l'étape finale.

7. Sous Propriété des objets, pour désactiver ou activer ACLs et contrôler la propriété des objets chargés dans votre bucket, sélectionnez l'un des paramètres suivants :

   ACLs handicapé

   - Application par le propriétaire du compartiment (par défaut) : ACLs cette option est désactivée, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment à usage général et en a le contrôle total. ACLs n'affectent plus les autorisations d'accès aux données du compartiment à usage général S3. Le compartiment utilise des stratégies exclusivement pour définir le contrôle des accès.

     Par défaut, ACLs sont désactivés. La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

   ACLs enabled

   - Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.

     Si vous appliquez le paramètre Propriétaire du compartiment préféré, pour exiger que tous les chargements Amazon S3 incluent la liste ACL prédéfinie `bucket-owner-full-control`, vous pouvez ajouter une politique de compartiment qui autorise uniquement les chargements d'objets utilisant cette liste ACL.
   - Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

> **Note**
>
> Le paramètre par défaut est Propriétaire du compartiment appliqué. Pour appliquer le paramètre par défaut et le maintenir ACLs désactivé, seule l'`s3:CreateBucket`autorisation est nécessaire. Pour l'activer ACLs, vous devez avoir l'`s3:PutBucketOwnershipControls`autorisation.

8. Dans Paramètres de blocage de l'accès public pour ce compartiment, choisissez les paramètres Bloquer l'accès public que vous souhaitez appliquer au compartiment.

   Par défaut, les quatre paramètres de blocage de l'accès public sont activés. Nous vous recommandons de maintenir tous les paramètres activés, sauf si vous savez que vous devez en désactiver un ou plusieurs pour votre cas d'utilisation spécifique. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

   > **Note**
   >
   > Pour activer tous les paramètres de blocage de l'accès public, seule l'autorisation `s3:CreateBucket` est requise. Pour désactiver les paramètres de blocage de l'accès public, vous devez disposer de l'autorisation `s3:PutBucketPublicAccessBlock`.

9. (Facultatif) Par défaut, le versionnement des compartiments est désactivé. La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans un même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment. Le contrôle de version permet de récupérer facilement les données en cas d'action involontaire d'un utilisateur ou de défaillance applicative. Pour plus d'informations sur la gestion des versions, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

   Pour activer le versionnement sur votre compartiment, choisissez Enable.

10. (Facultatif) Sous Tags (Balises), vous pouvez choisir d'ajouter des balises à votre compartiment. Avec la répartition des AWS coûts, vous pouvez utiliser des balises de compartiment pour annoter la facturation liée à l'utilisation d'un compartiment. Une balise correspond à une paire clé-valeur représentant un libellé que vous affectez à un compartiment. Pour de plus amples informations, veuillez consulter the section called "Utilisation des balises de répartition des coûts".

Pour ajouter une balise de compartiment, saisissez une Key (Clé) et éventuellement une Value (Valeur), puis choisissez Add Tag (Ajouter une balise).

11. Pour configurer le chiffrement par défaut, sous Type de chiffrement, sélectionnez l'une des options suivantes :

    - Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
    - Chiffrement côté serveur avec AWS Key Management Service clés (SSE-KMS)
    - Chiffrement double couche côté serveur avec clés AWS Key Management Service (AWS KMS) (DSSE-KMS)

    > **Important**
    >
    > Si vous utilisez l'option SSE-KMS ou DSSE-KMS pour votre configuration de chiffrement par défaut, vous êtes soumis au quota de demandes par seconde (RPS) de. AWS KMS Pour plus d'informations sur les AWS KMS quotas et sur la manière de demander une augmentation de quota, consultez la section Quotas dans le guide du AWS Key Management Service développeur.

    Les buckets et les nouveaux objets sont chiffrés en utilisant le chiffrement côté serveur avec les clés gérées Amazon S3 (SSE-S3) comme niveau de base de configuration de chiffrement. Pour plus d'informations sur le chiffrement par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Pour en savoir plus sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

    Pour plus d'informations sur l'utilisation du chiffrement côté serveur pour chiffrer vos données, consultez. the section called “Chiffrement des données”

12. Si vous avez choisi le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3) ou le chiffrement côté serveur double couche avec des clés () AWS Key Management Service (DSSE-KMS AWS KMS), procédez comme suit :

    a. Sous CléAWS KMS , spécifiez votre clé KMS de l'une des manières suivantes :

        - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans la liste des clés disponibles.

La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

- Pour saisir l'ARN de la clé KMS, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de votre clé KMS dans le champ qui s'affiche.
- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

  Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS appartenant à un autre compte, vous devez d'abord être autorisé à utiliser la clé, puis saisir l'ARN de la clé KMS. Pour plus d'informations sur les autorisations entre comptes pour les clés KMS, consultez la section Création de clés KMS utilisables par d'autres comptes dans le guide du AWS Key Management Service développeur. Pour en savoir plus sur SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS). Pour en savoir plus sur DSSE-KMS, consultez the section called "Chiffrement double couche côté serveur (DSSE-KMS)".
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez Identification des clés KMS symétriques et asymétriques dans le Guide du développeur AWS Key Management Service .

b. Lorsque vous configurez votre compartiment pour utiliser le chiffrement par défaut avec SSE-KMS, vous pouvez également utiliser les clés de compartiment S3. Les clés de compartiment S3 réduisent le coût du chiffrement en diminuant le trafic de demandes

d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3. Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS.

Par défaut, les clés de compartiment S3 sont activées dans la console Amazon S3. Nous vous recommandons de laisser les clés de compartiment S3 activées pour réduire vos coûts. Pour désactiver les clés de compartiment S3 pour votre compartiment, sous Clé de compartiment, choisissez Disable.

13. (Facultatif) S3 Object Lock permet de protéger les nouveaux objets contre la suppression ou le remplacement. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet. Si vous souhaitez activer S3 Object Lock, procédez comme suit :

    a. Choisissez Paramètres avancés.

    > **Important**
    >
    > L'activation d'Object Lock active automatiquement le versionnement du bucket. Après avoir activé et créé le bucket avec succès, vous devez également configurer les paramètres de rétention par défaut et de conservation légale d'Object Lock dans l'onglet Propriétés du bucket.

    b. Pour activer le verrouillage d'objets, choisissez Enable (Activer), lisez l'avertissement qui s'affiche et confirmez-le.

    > **Note**
    >
    > Pour créer un bucket activé pour Object Lock, vous devez disposer des autorisations suivantes : `s3:CreateBuckets3:PutBucketVersioning`, `ets3:PutBucketObjectLockConfiguration`.

14. Choisissez Créer un compartiment.

À l'aide du AWS SDKs

Lorsque vous utilisez le AWS SDKs pour créer un bucket à usage général, vous devez créer un client, puis utiliser le client pour envoyer une demande de création d'un bucket. En tant que bonne

pratique, vous devez créer votre client et votre compartiment dans la même Région AWS. Si vous ne spécifiez pas de région lorsque vous créez un client ou un compartiment, Amazon S3 utilise USA Est (Virginie du Nord), la région par défaut. Si vous souhaitez limiter la création du bucket à un paramètre spécifique Région AWS, utilisez la clé de LocationConstraintcondition.

Pour créer un client permettant d'accéder à un point de terminaison à double pile, vous devez spécifier un Région AWS. Pour plus d'informations, consultez Utilisation des points de terminaison à double pile Amazon S3 dans la Référence d'API Amazon S3. Pour obtenir la liste des points Régions AWS de terminaison et quotas Amazon Simple Storage Service disponibles dans le Références générales AWS.

Lorsque vous créez un client, la Région est mappée au point de terminaison spécifique à la Région. Le client utilise ce point de terminaison pour communiquer avec Amazon S3 : `s3.region.amazonaws.com`. Si votre Région a été lancée après le 20 mars 2019, votre client et votre compartiment doivent se trouver dans la même Région. Par conséquent, vous pouvez utiliser un client dans la Région USA Est (Virginie du Nord) pour créer un compartiment dans n'importe quelle Région lancée avant le 20 mars 2019. Pour de plus amples informations, veuillez consulter Points de terminaison hérités.

Ces exemples de code AWS SDK exécutent les tâches suivantes :

- Créer un client en indiquant explicitement une Région AWS : dans l'exemple, le client utilise le point de terminaison `s3.us-west-2.amazonaws.com` pour communiquer avec Amazon S3. Vous pouvez spécifier n'importe quelle Région AWS. Pour en obtenir la liste Régions AWS, voir Régions et points de terminaison dans le manuel de référence AWS général.
- Envoyer une demande de création de compartiment en indiquant uniquement un nom de compartiment : le client envoie une demande à Amazon S3 pour créer le compartiment dans la région où vous avez créé un client.
- Récupérez les informations relatives à l'emplacement du compartiment : Amazon S3 stocke les informations relatives à l'emplacement du compartiment dans la sous-ressource de localisation associée au compartiment.

Pour des exemples de AWS SDK supplémentaires et des exemples dans d'autres langages, consultez la section Utilisation CreateBucket avec un AWS SDK ou une CLI dans le manuel Amazon Simple Storage Service API Reference.

Java

Example Créez un compartiment utilisant un identifiant unique global (GUID) dans le nom du compartiment

L'exemple suivant vous montre comment créer un avec un GUID à la fin du nom du compartiment dans la région USA Est (Virginie du Nord) (`us-east-1`) en utilisant le AWS SDK pour Java. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations. Pour plus d'informations sur les autres AWS SDKs, voir Outils sur lesquels s'appuyer AWS.

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.CreateBucketRequest;

import java.util.List;
import java.util.UUID;

public class CreateBucketWithUUID {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.US_EAST_1).build();
        String bucketName = "amzn-s3-demo-bucket" +
 UUID.randomUUID().toString().replace("-", "");
        CreateBucketRequest createRequest = new CreateBucketRequest(bucketName);
        System.out.println(bucketName);
        s3.createBucket(createRequest);
    }
}
```

Example Création d'un compartiment à usage général

Cet exemple vous montre comment créer un compartiment Amazon S3 à l'aide du AWS SDK pour Java. Pour obtenir des instructions sur la création et le test d'un échantillon de travail, consultez le guide du AWS SDK for Java 2.x développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
```

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.GetBucketLocationRequest;

import java.io.IOException;

public class CreateBucket2 {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            if (!s3Client.doesBucketExistV2(bucketName)) {
                // Because the CreateBucketRequest object doesn't specify a region,
 the
                // bucket is created in the region specified in the client.
                s3Client.createBucket(new CreateBucketRequest(bucketName));

                // Verify that the bucket was created by retrieving it and checking
 its
                // location.
                String bucketLocation = s3Client.getBucketLocation(new
 GetBucketLocationRequest(bucketName));
                System.out.println("Bucket location: " + bucketLocation);
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Pour plus d'informations sur la création et le test d'un échantillon fonctionnel, consultez le manuel de AWS référence de l'API du SDK for .NET Version 3.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using Amazon.S3.Util;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CreateBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CreateBucketAsync().Wait();
        }

        static async Task CreateBucketAsync()
        {
            try
            {
                if (!(await AmazonS3Util.DoesS3BucketExistAsync(s3Client,
 bucketName)))
                {
                    var putBucketRequest = new PutBucketRequest
                    {
                        BucketName = bucketName,
                        UseClientRegion = true
                    };
```

```
                    PutBucketResponse putBucketResponse = await
 s3Client.PutBucketAsync(putBucketRequest);
                }
                // Retrieve the bucket location.
                string bucketLocation = await FindBucketLocationAsync(s3Client);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
        static async Task<string> FindBucketLocationAsync(IAmazonS3 client)
        {
            string bucketLocation;
            var request = new GetBucketLocationRequest()
            {
                BucketName = bucketName
            };
            GetBucketLocationResponse response = await
 client.GetBucketLocationAsync(request);
            bucketLocation = response.Location.ToString();
            return bucketLocation;
        }
    }
}
```

Ruby

Pour plus d'informations sur la création et le test d'un échantillon fonctionnel, consultez le AWS SDK pour Ruby - Version 3.

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 bucket actions.
class BucketCreateWrapper
  attr_reader :bucket
```

```
  # @param bucket [Aws::S3::Bucket] An Amazon S3 bucket initialized with a name.
 This is a client-side object until
  #                                 create is called.
  def initialize(bucket)
    @bucket = bucket
  end

  # Creates an Amazon S3 bucket in the specified AWS Region.
  #
  # @param region [String] The Region where the bucket is created.
  # @return [Boolean] True when the bucket is created; otherwise, false.
  def create?(region)
    @bucket.create(create_bucket_configuration: { location_constraint: region })
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't create bucket. Here's why: #{e.message}"
    false
  end

  # Gets the Region where the bucket is located.
  #
  # @return [String] The location of the bucket.
  def location
    if @bucket.nil?
      'None. You must create a bucket before you can get its location!'
    else
      @bucket.client.get_bucket_location(bucket: @bucket.name).location_constraint
    end
  rescue Aws::Errors::ServiceError => e
    "Couldn't get the location of #{@bucket.name}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  region = "us-west-2"
  wrapper = BucketCreateWrapper.new(Aws::S3::Bucket.new("amzn-s3-demo-bucket-
#{Random.uuid}"))
  return unless wrapper.create?(region)

  puts "Created bucket #{wrapper.bucket.name}."
  puts "Your bucket's region is: #{wrapper.location}"
end
```

```
run_demo if $PROGRAM_NAME == __FILE__
```

À l'aide du AWS CLI

L' AWS CLI exemple suivant crée un bucket à usage général dans la région USA Ouest (Californie du Nordus-west-1) () avec un exemple de nom de bucket utilisant un identifiant global unique (GUID). Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3api create-bucket \
    --bucket amzn-s3-demo-bucket1$(uuidgen | tr -d - | tr '[:upper:]' '[:lower:]' ) \
    --region us-west-1 \
    --create-bucket-configuration LocationConstraint=us-west-1
```

Pour plus d'informations et d'autres exemples, consultez create-bucketla référence des AWS CLI commandes.

Afficher les propriétés d'un bucket S3 à usage général

Vous pouvez consulter les propriétés de n'importe quel compartiment Amazon S3 que vous possédez. Il s'agit notamment des paramètres suivants :

- Versionnage des compartiments : conservez plusieurs versions d'un objet dans un compartiment à usage général en utilisant le versionnement. Par défaut, la gestion des versions est désactivée pour un nouveau compartiment. Pour plus d'informations sur l'activation de la gestion des versions, consultez Activation de la gestion des versions sur les compartiments.
- Balises — Dans le cadre de la répartition des AWS coûts, vous pouvez utiliser des balises de compartiment pour annoter la facturation relative à l'utilisation d'un compartiment à usage général. Une balise correspond à une paire clé-valeur représentant un libellé que vous affectez à un compartiment. Pour de plus amples informations, veuillez consulter Utilisation des balises de répartition des coûts pour les compartiments S3.
- Default encryption (Chiffrement par défaut) – L'activation du chiffrement par défaut vous permet de chiffrer automatiquement côté serveur. Amazon S3 chiffre un objet avant de l'enregistrer sur un disque et déchiffre l'objet quand vous le téléchargez. Pour de plus amples informations, veuillez consulter Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.

- Journalisation des accès au serveur : obtenez des enregistrements détaillés des demandes adressées à votre compartiment à usage général grâce à la journalisation des accès au serveur. Par défaut, Amazon S3 ne collecte pas les journaux d'accès au serveur. Pour plus d'informations sur l'activation de la journalisation des accès au serveur, consultez Activation de la journalisation des accès au serveur Amazon S3.
- AWS CloudTrail événements liés aux données : permet CloudTrail de consigner les événements liés aux données. Par défaut, les suivis ne consignent pas les événements de données. Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations, consultez Consignation d'événements de données pour les journaux d'activité dans le Guide de l'utilisateur AWS CloudTrail .
- Notifications d'événements — Activez certains événements de compartiment à usage général Amazon S3 pour envoyer des messages de notification à une destination chaque fois que ces événements se produisent. Pour de plus amples informations, veuillez consulter Activation et configuration des notifications d'événements à l'aide de la console Amazon S3.
- Transfer acceleration (Accélération de transfert) – Activez un transfert rapide, facile et sécurisé de fichiers à grande distance entre votre client et un compartiment S3. Pour plus d'informations sur l'activation de l'accélération du transfert, consultez Activation et utilisation de S3 Transfer Acceleration.
- Verrouillage d'objet : utilisez le verrouillage d'objet S3 pour empêcher qu'un objet soit supprimé ou remplacé sur une période déterminée ou indéfinie. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.
- Paiement par le demandeur : activez le paiement par le demandeur si vous souhaitez que le demandeur (plutôt que le propriétaire du compartiment à usage général) paie les demandes et les transferts de données. Pour de plus amples informations, veuillez consulter Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation.
- Static website hosting (Hébergement de site web statique) – Vous pouvez héberger un site web statique dans Amazon S3. Pour de plus amples informations, veuillez consulter Hébergement d'un site Web statique à l'aide d'Amazon S3.

Vous pouvez afficher les propriétés du compartiment à l'aide de AWS Management Console AWS CLI, ou AWS SDKs

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment dont vous souhaitez consulter les propriétés.
4. Choisissez l'onglet Propriétés.
5. Sur la page Propriétés, vous pouvez configurer les propriétés ci-dessus pour le compartiment.

À l'aide du AWS CLI

Consultez les propriétés du bucket à l'aide du AWS CLI

Les commandes suivantes montrent comment vous pouvez utiliser le AWS CLI pour répertorier les différentes propriétés de compartiment à usage général.

La commande suivante renvoie l'ensemble de balises associé au compartiment *amzn-s3-demo-bucket1*. Pour plus d'informations sur les balises des compartiments, consultez Utilisation des balises de répartition des coûts pour les compartiments S3.

```
aws s3api get-bucket-tagging --bucket amzn-s3-demo-bucket1
```

Pour plus d'informations et des exemples, consultez get-bucket-tagging dans la Référence des commandes de l'AWS CLI .

La commande suivante renvoie l'état de gestion des versions du compartiment *amzn-s3-demo-bucket1*. Pour plus d'informations sur la gestion des versions des compartiments, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

```
aws s3api get-bucket-versioning --bucket amzn-s3-demo-bucket1
```

Pour plus d'informations et des exemples, consultez get-bucket-versioning dans la Référence des commandes de l'AWS CLI .

La commande suivante renvoie la configuration de chiffrement par défaut du compartiment *amzn-s3-demo-bucket1*. Par défaut, tous les compartiments ont un niveau de chiffrement standard qui utilise le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3). Pour plus d'informations sur le chiffrement des compartiments par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

Pour plus d'informations et des exemples, consultez get-bucket-encryption dans la Référence des commandes de l'AWS CLI .

La commande suivante renvoie la configuration des notifications du compartiment *amzn-s3-demo-bucket1*. Pour plus d'informations sur les notifications d'événements des compartiments, consultez Notifications d'événements Amazon S3.

```
aws s3api get-bucket-notification-configuration --bucket amzn-s3-demo-bucket1
```

Pour plus d'informations et des exemples, consultez get-bucket-notification-configuration dans la Référence des commandes de l'AWS CLI .

La commande suivante renvoie l'état de journalisation du compartiment *amzn-s3-demo-bucket1*. Pour plus d'informations sur la journalisation des compartiments, consultez Enregistrement de demandes avec journalisation des accès au serveur.

```
aws s3api get-bucket-logging --bucket amzn-s3-demo-bucket1
```

Pour plus d'informations et des exemples, consultez get-bucket-logging dans la Référence des commandes de l'AWS CLI .

À l'aide du AWS SDKs

Pour des exemples expliquant comment renvoyer des propriétés de bucket à usage général avec le AWS SDKs, telles que le versionnement, les balises, etc., consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Répertorier les compartiments à usage général d'Amazon S3

Pour renvoyer une liste des buckets à usage général que vous possédez, vous pouvez utiliser ListBuckets. Vous pouvez répertorier vos compartiments à l'aide de la console Amazon S3, du

AWS Command Line Interface, ou du AWS SDKs. Pour les `ListBuckets` demandes utilisant l'API REST AWS CLI AWS SDKs,, et Amazon S3, Comptes AWS qui utilisent le quota de service par défaut pour les compartiments (10 000 compartiments), prennent en charge les demandes paginées et non paginées. Quel que soit le nombre de compartiments présents dans votre compte, vous pouvez créer des formats de page compris entre 1 et 10 000 compartiments pour afficher tous vos compartiments. Pour les demandes paginées, les `ListBuckets` demandes renvoient à la fois le nom du compartiment et le nom correspondant Régions AWS à chaque compartiment. Les exemples suivants AWS Command Line Interface et AWS ceux du SDK vous montrent comment utiliser la pagination dans votre `ListBuckets` demande. Notez que certains AWS SDKs facilitent la pagination.

Autorisations

Pour répertorier tous vos compartiments à usage général, vous devez en avoir l'`s3:ListAllMyBuckets`autorisation. Si vous rencontrez une erreur `HTTP Access Denied (403 Forbidden)`, consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3.

> **Important**
>
> Nous vous recommandons vivement de n'utiliser que des demandes `ListBuckets` paginées. Les demandes `ListBuckets` non paginées ne sont prises en charge que pour les Comptes AWS dont le quota de compartiments à usage général par défaut a été défini sur 10 000. Si vous avez un quota de compartiments à usage général approuvé supérieur à 10 000, vous devez envoyer des demandes `ListBuckets` paginées pour répertorier les compartiments de votre compte. Toutes les `ListBuckets` demandes non paginées seront rejetées si le quota de Comptes AWS compartiments à usage général est supérieur à 10 000.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans l'onglet Compartiments à usage général, vous pouvez voir la liste de vos compartiments à usage général.
4. Pour rechercher des compartiments par nom, entrez un nom de compartiment dans le champ Rechercher des compartiments par nom.

À l'aide du AWS CLI

AWS CLI Pour générer une liste de compartiments à usage général, vous pouvez utiliser les `list-buckets` commandes `ls` ou. Les exemples suivants montrent comment créer une demande `list-buckets` paginée et une demande `ls` non paginée. Pour utiliser ces exemples, remplacez le*`user input placeholders`*.

Example — Afficher tous les compartiments de votre compte avec **`ls`** (appel non paginé)

L'exemple de commande suivant répertorie tous les compartiments à usage général de votre compte en un seul appel non paginé. Cet appel renvoie une liste de tous les compartiments de votre compte (jusqu'à 10 000 résultats) :

```
$ aws s3 ls
```

Pour plus d'informations et pour obtenir des exemples, consultez Liste des compartiments et des objets.

Example — Afficher tous les compartiments de votre compte avec **`ls`** (appel paginé)

L'exemple de commande suivant effectue un ou plusieurs appels paginés pour afficher tous les compartiments à usage général de votre compte. Il renvoie 100 compartiments par page :

```
$ aws s3 ls --page-size 100
```

Pour plus d'informations et pour obtenir des exemples, consultez Liste des compartiments et des objets.

Example — Afficher tous les compartiments de votre compte (appel paginé)

L'exemple suivant fournit une commande `list-buckets` paginée qui répertorie tous les compartiments à usage général de votre compte. Les options `--max-items` et `--page-size` limitent le nombre de compartiments répertoriés à 100 par page.

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100
```

Si le nombre d'éléments en sortie (`--max-items`) est inférieur au nombre total d'éléments renvoyés par les appels d'API sous-jacents, la sortie inclut un jeton de continuation, spécifié par l'argument `starting-token`. Vous pourrez transmettre ce jeton dans une commande ultérieure pour extraire le prochain ensemble d'éléments. L'exemple suivant montre comment utiliser la valeur `starting-token` renvoyée par l'exemple précédent. Vous pouvez spécifier `starting-code` pour récupérer les 100 prochains compartiments.

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
    --starting-token eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZV9hbW91bnQiOiAxfQ==
```

Example — Liste tous les buckets dans un Région AWS (paginé)

L'exemple de commande suivant utilise le paramètre `--bucket-region` pour répertorier jusqu'à 100 compartiments situés dans la région `us-east-2` pour un compte. Les demandes adressées à un point de terminaison régional différent de la valeur spécifiée dans le paramètre `--bucket-region` ne sont pas prises en charge. Par exemple, si vous souhaitez limiter la réponse aux compartiments qui se trouvent dans la région `us-east-2`, vous devez envoyer votre demande à un point de terminaison dans `us-east-2`.

```
$ aws s3api list-buckets /
    --region us-east-2 /
    --max-items 100 /
    --page-size 100 /
    --bucket-region us-east-2
```

Example — Afficher tous les compartiments commençant par un préfixe de nom de compartiment spécifique (appel paginé)

L'exemple de commande suivant répertorie jusqu'à 100 compartiments dont le nom commence par le préfixe *`amzn-s3-demo-bucket`*.

```
$ aws s3api list-buckets /
    --max-items 100 /
    --page-size 100 /
    --prefix amzn-s3-demo-bucket
```

À l'aide du AWS SDKs

Les exemples suivants vous montrent comment répertorier vos compartiments à usage général à l'aide du AWS SDKs

SDK for Python

Example — ListBuckets demande (paginée)

```
import boto3

s3 = boto3.client('s3')
response = s3.list_buckets(MaxBuckets=100)
```

Example — ListBuckets réponse (paginée)

```
import boto3

s3 = boto3.client('s3')
response =
 s3.list_buckets(MaxBuckets=1,ContinuationToken="eyJNYXJrZXIiOiBudWxsLCAiYm90b190cnVuY2F0ZVS
```

SDK for Java

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.Bucket;
import com.amazonaws.services.s3.model.ListBucketsPaginatedRequest;
import com.amazonaws.services.s3.model.ListBucketsPaginatedResult;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        final AmazonS3 s3 =
 AmazonS3ClientBuilder.standard().withRegion(Regions.DEFAULT_REGION).build();
        ListBucketsPaginatedRequest listBucketsPaginatedRequest = new
 ListBucketsPaginatedRequest().withMaxBuckets(1);
        ListBucketsPaginatedResult listBucketsPaginatedResult =
 s3.listBuckets(listBucketsPaginatedRequest);
        List<Bucket> buckets = listBucketsPaginatedResult.getBuckets();
```

```
        System.out.println("Your Amazon S3 buckets are:");
        for (Bucket b : buckets) {
            System.out.println("* " + b.getName() + " region: " + b.getRegion());
        }
        System.out.println("continuation token: " +
 listBucketsPaginatedResult.getContinuationToken());
    }
}
```

SDK for Java 2.x

```
import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.Bucket;
import software.amazon.awssdk.services.s3.model.ListBucketsRequest;
import software.amazon.awssdk.services.s3.model.ListBucketsResponse;

import java.util.List;

public class ListBuckets {
    public static void main(String[] args) {
        // Create an S3 client
        S3Client s3 = S3Client.builder()
                .region(Region.US_EAST_1) // Replace with your preferred region
                .credentialsProvider(DefaultCredentialsProvider.create())
                .build();

        try {
            // List buckets
            ListBucketsRequest listBucketsRequest = ListBucketsRequest.builder()
                    .maxBuckets(10)
                    .build();
            ListBucketsResponse listBucketsResponse =
 s3.listBuckets(listBucketsRequest);
            List<Bucket> buckets = listBucketsResponse.buckets();

            // Print bucket names
            System.out.println("Your Amazon S3 buckets are:");
            for (Bucket bucket : buckets) {
                System.out.println(bucket.name());
                System.out.println(bucket.getBucketRegion());
            }
```

```
        } catch (Exception e) {
            System.err.println("Error listing buckets: " + e.getMessage());
            e.printStackTrace();
        } finally {
            // Close the S3 client to release resources
            s3.close();
        }
    }
}
```

SDK for Go

```
package main
import (
 "context"
 "fmt"
 "log"
 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/config"
 "github.com/aws/aws-sdk-go-v2/service/s3"
)
func main() {
 cfg, err := config.LoadDefaultConfig(context.TODO(), config.WithRegion("us-
east-2"))
 if err != nil {
  log.Fatal(err)
 }
 client := s3.NewFromConfig(cfg)
 maxBuckets := 1000
 resp, err := client.ListBuckets(context.TODO(), management
 portals3.ListBucketsInput{MaxBuckets: aws.Int32(int32(maxBuckets))})
 if err != nil {
  log.Fatal(err)
 }
 fmt.Println("S3 Buckets:")
 for _, bucket := range resp.Buckets {
     fmt.Println("- Name:", *bucket.Name)
     fmt.Println("-BucketRegion", *bucket.BucketRegion)
 }
 fmt.Println(resp.ContinuationToken == nil)
 fmt.Println(resp.Prefix == nil)
}
```

Vidange d'un seau à usage général

Vous pouvez vider le contenu d'un compartiment à usage général à l'aide de la console Amazon S3 AWS SDKs, ou AWS Command Line Interface (AWS CLI). Lorsque vous videz un compartiment à usage général, vous supprimez tous les objets, mais vous le conservez. Après avoir vidé un compartiment, les éléments supprimés ne peuvent être restaurés. Les objets ajoutés au compartiment pendant que l'action est en cours, risquent d'être supprimés. Tous les objets (y compris toutes les versions d'objets et les marqueurs de suppression) du compartiment doivent être supprimés avant que le compartiment lui-même ne puisse être supprimé.

Lorsque vous videz un compartiment à usage général pour lequel le contrôle de version S3 est activé ou suspendu, toutes les versions de tous les objets du compartiment sont supprimées. Pour de plus amples informations, veuillez consulter Utiliser des objets dans un compartiment activé pour la gestion des versions.

Lorsque vous videz votre bucket, nous vous recommandons de supprimer également tous les téléchargements partitionnés incomplets. Vous pouvez utiliser les chargements partitionnés pour charger des objets de très grande taille (jusqu'à 5 To) en tant qu'ensemble de parties pour améliorer le débit et accélérer la récupération suite à des problèmes réseau. Dans les cas où le processus de chargement partitionné ne se termine pas, les parties incomplètes restent dans le compartiment (dans un état inutilisable). Ces parties incomplètes entraînent des coûts de stockage jusqu'à la fin du processus de chargement ou jusqu'à leur suppression. Pour de plus amples informations, veuillez consulter Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Il est recommandé de configurer des règles de cycle de vie pour faire expirer les objets et les chargements partitionnés incomplets datant de plus d'un certain nombre de jours. Lorsque vous créez votre règle de cycle de vie pour faire expirer les chargements partitionnés non terminés, nous recommandons un délai de 7 jours comme point de départ. Pour de plus amples informations, veuillez consulter Définition d'une configuration du cycle de vie S3 sur un compartiment.

L'expiration du cycle de vie étant un processus asynchrone, l'exécution de la règle peut prendre quelques jours avant que votre compartiment ne soit vide. Après la première exécution de la règle par Amazon S3, tous les objets éligibles à l'expiration sont marqués comme devant être supprimés. Les objets marqués comme devant être supprimés ne vous sont plus facturés. Pour plus d'informations, consultez Comment vider un compartiment Amazon S3 à l'aide d'une règle de configuration du cycle de vie ?.

Utilisation de la console S3

Vous pouvez utiliser la console Amazon S3 pour vider un compartiment à usage général, ce qui supprime tous les objets du compartiment sans supprimer le compartiment.

Pour vider un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, sélectionnez l'option à côté du nom du compartiment que vous souhaitez vider, puis choisissez Empty.
4. Sur la page Empty bucket (Vider le compartiment), confirmez que vous souhaitez vider le compartiment en saisissant le nom de ce dernier dans le champ de texte, puis choisissez Empty (Vider).
5. Surveillez la progression du processus de vidage du compartiment sur la page Vider le compartiment : état.

À l'aide du AWS CLI

Vous pouvez vider un bucket à usage général en utilisant le AWS CLI uniquement si la gestion des versions des compartiments n'est pas activée sur le bucket. Si le contrôle de version n'est pas activé, vous pouvez utiliser la AWS CLI commande `rm` (remove) avec le `--recursive` paramètre pour vider le compartiment (ou supprimer un sous-ensemble d'objets avec un préfixe de nom de clé spécifique).

La commande `rm` suivante supprime les objets ayant un préfixe de nom de clé `doc`, par exemple, `doc/doc1` et `doc/doc2`.

```
$ aws s3 rm s3://bucket-name/doc --recursive
```

Utilisez la commande suivante pour supprimer tous les objets sans spécifier un préfixe.

```
$ aws s3 rm s3://bucket-name --recursive
```

Pour plus d'informations, consultez Utilisation des commandes S3 de haut niveau avec l' AWS CLI dans le Guide de l'utilisateur de l'AWS Command Line Interface .

> **Note**
>
> Vous ne pouvez pas supprimer des objets d'un compartiment pour lequel la gestion des versions est activée. Amazon S3 ajoute un marqueur de suppression lorsque vous supprimez un objet, à l'instar de cette commande. Pour plus d'informations sur la gestion des versions des compartiments S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour vider un compartiment à usage général ou supprimer un sous-ensemble d'objets dotés d'un préfixe de nom de clé spécifique.

Pour un exemple de la façon de vider un bucket en utilisant AWS SDK pour Java, reportez-vous à la sectionSupprimer un bucket à usage général. Le code supprime tous les objets, que le compartiment soit activé ou non pour la gestion des versions, puis il supprime le compartiment. Pour simplement vider le compartiment, assurez-vous de supprimer l'instruction de suppression du compartiment.

Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez la section Outils pour Amazon Web Services.

Utilisation de la configuration du cycle de vie

Pour vider un grand compartiment à usage général, nous vous recommandons d'utiliser une règle de configuration S3 Lifecycle. L'expiration du cycle de vie étant un processus asynchrone, l'exécution de la règle peut mettre plusieurs jours à vider le compartiment. Après la première exécution de la règle par Amazon S3, tous les objets éligibles à l'expiration sont marqués comme devant être supprimés. Les objets marqués comme devant être supprimés ne vous sont plus facturés. Pour plus d'informations, consultez Comment vider un compartiment Amazon S3 à l'aide d'une règle de configuration du cycle de vie ?.

Si vous utilisez une configuration de cycle de vie pour vider votre compartiment, la configuration doit inclure des versions actuelles, des versions anciennes, des marqueurs de suppression et des chargements partitionnés incomplets.

Vous pouvez ajouter des règles de configuration du cycle de vie pour que tous les objets ou un sous-ensemble d'objets ayant un préfixe de nom de clé spécifique expirent. Par exemple, pour supprimer tous les objets dans un compartiment, vous pouvez configurer une règle du cycle de vie pour que les objets expirent un jour après leur création.

Amazon S3 prend en charge une règle de cycle de vie de compartiment que vous pouvez utiliser pour arrêter les chargements partitionnés s'ils n'aboutissent pas au bout du nombre de jours spécifié après leur lancement. Nous vous recommandons de configurer cette règle de cycle de vie afin de réduire vos coûts de stockage. Pour plus d'informations, consultez Configuration d'une configuration de cycle de vie de compartiment pour supprimer les chargements partitionnés incomplets.

Pour plus d'informations sur l'utilisation d'une configuration de cycle de vie pour vider un compartiment, consultez Définition d'une configuration du cycle de vie S3 sur un compartiment et Objets en cours d'expiration.

Vidange d'un godet à usage général avec une configuration AWS CloudTrail

AWS CloudTrail suit les événements de données au niveau des objets dans un compartiment à usage général Amazon S3, tels que la suppression d'objets. Si vous utilisez un compartiment à usage général comme destination pour enregistrer vos CloudTrail événements et que vous supprimez des objets de ce même compartiment, il est possible que vous créiez de nouveaux objets en vidant votre compartiment. Pour éviter cela, bloquez vos AWS CloudTrail sentiers. Pour plus d'informations sur la façon d'empêcher l'enregistrement d'événements dans vos CloudTrail sentiers, consultez la section Désactiver la journalisation d'un sentier dans le guide de AWS CloudTrail l'utilisateur.

Une autre alternative pour empêcher l'ajout de CloudTrail sentiers au bucket consiste à ajouter une `s3:PutObject` déclaration de refus à votre politique de bucket. Si vous souhaitez stocker ultérieurement de nouveaux objets dans le compartiment, vous devrez supprimer cette instruction de refus `s3:PutObject`. Pour plus d'informations, consultez Opérations d'objet et Éléments de politique JSON IAM : Effect dans le Guide de l'utilisateur IAM.

Supprimer un bucket à usage général

Vous pouvez supprimer un compartiment Amazon S3 à usage général vide. Pour plus d'informations sur le vidage d'un godet à usage général, consultezthe section called "Vidange d'un seau à usage général".

Vous pouvez supprimer un compartiment à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) AWS SDKs, de ou de l'API REST Amazon S3.

> **Important**
>
> Avant de supprimer un bucket à usage général, tenez compte des points suivants :

- les noms de bucket à usage général sont uniques au sein d'un espace de noms global. Si vous supprimez un compartiment, sachez qu'un autre Compte AWS peut utiliser le même nom de compartiment général pour un nouveau compartiment et peut donc potentiellement recevoir des demandes destinées au compartiment supprimé. Si vous souhaitez empêcher cela, ou si vous souhaitez continuer à utiliser le même nom de bucket, ne supprimez pas le bucket. Nous vous recommandons de vider le compartiment et de le conserver, et de bloquer toutes les demandes de compartiment selon les besoins. Pour les seaux qui ne sont plus utilisés activement, nous recommandons de vider le seau de tous les objets afin de minimiser les coûts tout en conservant le seau lui-même.
- Lorsque vous supprimez un compartiment à usage général, il se peut que celui-ci ne soit pas supprimé instantanément. Au lieu de cela, Amazon S3 met le compartiment en file d'attente pour le supprimer. Amazon S3 étant distribué sur l'ensemble du système Régions AWS, le processus de suppression prend du temps à se propager complètement et à garantir la cohérence dans l'ensemble du système.
- Si le compartiment héberge un site Web statique et que vous avez créé et configuré une zone hébergée Amazon Route 53 comme décrit dans Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53, vous devez nettoyer les paramètres de zone hébergée Route 53 qui sont associés au compartiment. Pour de plus amples informations, veuillez consulter Étape 2 : Supprimer la zone hébergée Route 53.
- Si le bucket reçoit des données de journal d'Elastic Load Balancing (ELB), nous vous recommandons d'arrêter la livraison des journaux ELB au bucket avant de le supprimer. Après que vous avez supprimé le compartiment, si un autre utilisateur crée un compartiment à l'aide du même nom, vos données de journaux peuvent potentiellement être remises à ce compartiment. Pour plus d'informations sur les journaux d'accès ELB, consultez les journaux d'accès de votre Classic Load Balancer dans le Guide de l'utilisateur pour les Classic Load Balancers et les journaux d'accès pour votre Application Load Balancer dans le Guide de l'utilisateur pour les Application Load Balancers.

Résolution des problèmes

Si vous ne parvenez pas à supprimer un compartiment Amazon S3 à usage général, prenez en compte les points suivants :

- Assurez-vous que le compartiment est vide : vous ne pouvez supprimer des compartiments que s'ils ne contiennent aucun objet. Assurez-vous que le seau est vide. Pour plus d'informations sur le vidage d'un bucket, consultezthe section called "Vidange d'un seau à usage général".
- Assurez-vous qu'aucun point d'accès n'est attaché : vous ne pouvez supprimer des compartiments que s'ils ne contiennent aucun point d'accès S3 ou multirégional associé au même compte. Avant de supprimer le compartiment, supprimez tous les points d'accès associés au même compte qui y sont attachés.
- Assurez-vous de disposer de l'**`s3:DeleteBucket`**autorisation : si vous ne pouvez pas supprimer un bucket, contactez votre administrateur IAM pour confirmer que vous disposez de l'`s3:DeleteBucket`autorisation. Pour plus d'informations sur l'affichage ou la mise à jour des autorisations IAM, consultez Modification des autorisations pour un utilisateur IAM dans le Guide de l'utilisateur IAM. Pour plus d'informations sur le dépannage, consultez the section called "Résolution des erreurs d'accès refusé (403 Forbidden)".
- Vérifiez les **`s3:DeleteBucket Deny`** instructions contenues dans les politiques de contrôle des AWS Organizations services (SCPs) et les politiques de contrôle des ressources (RCPs), SCPs et RCPs vous pouvez refuser l'autorisation de suppression d'un bucket. Pour plus d'informations, consultez Politiques de contrôle des services et Politiques de contrôle des ressources dans le Guide de l'utilisateur AWS Organizations .
- Vérifiez la présence de **`s3:DeleteBucket Deny`** déclarations dans votre politique de compartiment — Si vous disposez d'`s3:DeleteBucket`autorisations dans votre politique d'utilisateur ou de rôle IAM et que vous ne pouvez pas supprimer un compartiment, la politique de compartiment peut inclure une `Deny` instruction pour`s3:DeleteBucket`. Les compartiments créés par AWS Elastic Beanstalk ont une politique contenant cette instruction par défaut. Avant de pouvoir supprimer le compartiment, vous devez supprimer cette instruction ou la politique de compartiment.

Prérequis

Avant de pouvoir supprimer un bucket à usage général, vous devez le vider. Pour plus d'informations sur le vidage d'un bucket, consultezthe section called "Vidange d'un seau à usage général".

Utilisation de la console S3

Pour supprimer un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, sélectionnez le bouton d'option à côté du nom du compartiment que vous souhaitez supprimer, puis choisissez Supprimer en haut de la page.
4. Dans la page Supprimer le compartiment, confirmez que vous souhaitez supprimer le compartiment en saisissant le nom de ce dernier dans le champ de texte, puis choisissez Supprimer le compartiment.

> **Note**
>
> Si le compartiment contient des objets, videz-le avant de le supprimer en cliquant sur le bouton Compartiment vide dans l'alerte d'erreur Ce compartiment n'est pas vide et en suivant les instructions de la page Compartiment vide. Revenez ensuite à la page Delete bucket (Supprimer le compartiment) et supprimez le compartiment.

5. Pour vérifier que vous avez supprimé le bucket, ouvrez la liste des buckets à usage général et entrez le nom du bucket que vous avez supprimé. Si le compartiment est introuvable, votre suppression a réussi.

Utilisation du AWS SDK pour Java

L'exemple suivant montre comment vider et supprimer un compartiment à usage général à l'aide du AWS SDK pour Java. Le code supprime d'abord tous les objets du compartiment à usage général, puis il supprime le compartiment.

Pour des exemples dans d'autres langages, consultez la section Utilisation DeleteBucket avec un AWS SDK ou une CLI dans le manuel Amazon Simple Storage Service API Reference. Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez la section Outils pour Amazon Web Services.

Java

L'Javaexemple suivant supprime un compartiment contenant des objets. Il supprime tous les objets, puis il supprime le compartiment. L'exemple fonctionne pour les compartiments avec ou sans la gestion des versions activée.

> **Note**
>
> Pour les compartiments sans la gestion des versions activée, vous pouvez supprimer tous les objets directement, puis supprimer le compartiment. Pour les compartiments avec la gestion des versions activée, vous devez supprimer toutes les versions d'objet avant de supprimer le compartiment.

Pour obtenir des instructions sur la création et le test d'un échantillon de travail, consultez le guide du AWS SDK for Java 2.x développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.Iterator;

public class DeleteBucket2 {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Delete all objects from the bucket. This is sufficient
            // for unversioned buckets. For versioned buckets, when you attempt to
 delete
            // objects, Amazon S3 inserts
            // delete markers for all objects, but doesn't delete the object
 versions.
            // To delete objects from versioned buckets, delete all of the object
 versions
```

```
            // before deleting
            // the bucket (see below for an example).
            ObjectListing objectListing = s3Client.listObjects(bucketName);
            while (true) {
                Iterator<S3ObjectSummary> objIter =
objectListing.getObjectSummaries().iterator();
                while (objIter.hasNext()) {
                    s3Client.deleteObject(bucketName, objIter.next().getKey());
                }

                // If the bucket contains many objects, the listObjects() call
                // might not return all of the objects in the first listing. Check
to
                // see whether the listing was truncated. If so, retrieve the next
page of
                // objects
                // and delete them.
                if (objectListing.isTruncated()) {
                    objectListing = s3Client.listNextBatchOfObjects(objectListing);
                } else {
                    break;
                }
            }

            // Delete all object versions (required for versioned buckets).
            VersionListing versionList = s3Client.listVersions(new
ListVersionsRequest().withBucketName(bucketName));
            while (true) {
                Iterator<S3VersionSummary> versionIter =
versionList.getVersionSummaries().iterator();
                while (versionIter.hasNext()) {
                    S3VersionSummary vs = versionIter.next();
                    s3Client.deleteVersion(bucketName, vs.getKey(),
vs.getVersionId());
                }

                if (versionList.isTruncated()) {
                    versionList = s3Client.listNextBatchOfVersions(versionList);
                } else {
                    break;
                }
            }

            // After all objects and object versions are deleted, delete the bucket.
```

```
            s3Client.deleteBucket(bucketName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
 couldn't
            // parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

À l'aide du AWS CLI

Vous pouvez supprimer un bucket à usage général qui contient des objets à l'aide du AWS CLI si la gestion des versions n'est pas activée pour le bucket. Lorsque vous supprimez un compartiment contenant des objets, tous les objets qu'il contient sont définitivement supprimés, y compris les objets qui ont été transférés vers la classe de stockage S3 Glacier Flexible Retrieval.

Si la gestion des versions n'est pas activée dans votre bucket, vous pouvez utiliser la AWS CLI commande `rb` (remove bucket) avec le `--force` paramètre pour supprimer le bucket et tous les objets qu'il contient. Cette commande supprime d'abord tous les objets, puis le compartiment.

Si le contrôle de version est activé, l'utilisation de la `rb` commande avec le `--force` paramètre ne supprime pas les objets versionnés. La suppression du compartiment échoue donc car le compartiment n'est pas vide. Pour obtenir des informations sur la suppression d'objets versionnés, consultez Suppression des versions d'objet.

Pour utiliser la commande suivante, *`amzn-s3-demo-bucket`* remplacez-la par le nom du bucket que vous souhaitez supprimer :

```
$ aws s3 rb s3://amzn-s3-demo-bucket --force
```

Pour plus d'informations, consultez la section Utilisation de commandes S3 de haut niveau AWS Command Line Interface dans le guide de AWS Command Line Interface l'utilisateur.

Monter un compartiment Amazon S3 en tant que système de fichiers local

Mountpoint pour Amazon S3 est un client de fichiers open source à haut débit permettant de monter un compartiment Amazon S3 en tant que système de fichiers local. Avec Mountpoint, vos applications peuvent accéder aux objets stockés dans Amazon S3 par le biais d'opérations de système de fichiers, telles qu'ouvrir et lire. Mountpoint traduit automatiquement ces opérations en appels d'API d'objet S3, permettant à vos applications d'accéder au stockage et au débit élastiques d'Amazon S3 via une interface de fichier.

Mountpoint pour Amazon S3 est disponible pour une utilisation en production sur vos applications à lecture intensive à grande échelle : lacs de données, entraînement de machine learning, rendu d'images, simulation de véhicules autonomes, extraction, transformation et chargement (ETL), etc.

Mountpoint prend en charge les opérations de base de système de fichiers et peut lire des fichiers d'une taille maximale de 5 To. Il peut répertorier et lire des fichiers existants, et il peut en créer de nouveaux. Il ne peut pas modifier les fichiers existants ni supprimer de répertoires, et il ne prend pas en charge les liens symboliques ni le verrouillage de fichiers. Mountpoint est idéal pour les applications qui n'ont pas besoin de toutes les fonctionnalités d'un système de fichiers partagé et des autorisations de style POSIX, mais qui ont besoin du débit élastique d'Amazon S3 pour lire et écrire de grands jeux de données S3. Pour obtenir des détails, consultez Comportement du système de fichiers Mountpoint (langue française non garantie) sur GitHub. Pour les charges de travail nécessitant un support POSIX complet, nous recommandons Amazon FSx for Lustre et son support pour relier les buckets Amazon S3.

Mountpoint pour Amazon S3 est disponible uniquement pour les systèmes d'exploitation Linux. Vous pouvez utiliser Mountpoint pour accéder aux objets S3 dans toutes les classes de stockage, sauf S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, le niveau Archive Access de S3 Intelligent-Tiering et le niveau Deep Archive Access de S3 Intelligent-Tiering.

Rubriques

- Installation de Mountpoint
- Configuration et utilisation de Mountpoint
- Dépannage de Mountpoint

Installation de Mountpoint

Vous pouvez télécharger et installer des packages précréés de Mountpoint pour Amazon S3 à l'aide de la ligne de commande. Les instructions de téléchargement et d'installation de Mountpoint varient en fonction du système d'exploitation Linux que vous utilisez.

Rubriques

- Distributions basées sur RPM (Amazon Linux, Fedora, CentOS, RHEL)
- Distributions basées sur DEB (Debian, Ubuntu)
- Autres distributions Linux
- Vérification de la signature du package Mountpoint pour Amazon S3

Distributions basées sur RPM (Amazon Linux, Fedora, CentOS, RHEL)

1. Copiez l'URL de téléchargement suivante pour votre architecture.

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
   ```

   ARM64 (Graviton):

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm
   ```

2. Téléchargez le package Mountpoint pour Amazon S3. Remplacez *download-link* par l'URL de téléchargement appropriée indiquée à l'étape précédente.

   ```
   wget download-link
   ```

3. (Facultatif) Vérifiez l'authenticité et l'intégrité du fichier téléchargé. Tout d'abord, copiez l'URL de signature appropriée pour votre architecture.

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm.asc
   ```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.rpm.asc
```

Ensuite, consultez Vérification de la signature du package Mountpoint pour Amazon S3.

4. Installez le package à l'aide de la commande suivante :

```
sudo yum install ./mount-s3.rpm
```

5. Vérifiez que Mountpoint est correctement installé en saisissant la commande suivante :

```
mount-s3 --version
```

Vous devez voir des résultats similaires à ce qui suit :

```
mount-s3 1.3.1
```

Distributions basées sur DEB (Debian, Ubuntu)

1. Copiez l'URL de téléchargement pour votre architecture.

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb
```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb
```

2. Téléchargez le package Mountpoint pour Amazon S3. Remplacez *download-link* par l'URL de téléchargement appropriée indiquée à l'étape précédente.

```
wget download-link
```

3. (Facultatif) Vérifiez l'authenticité et l'intégrité du fichier téléchargé. Tout d'abord, copiez l'URL de signature pour votre architecture.

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.deb.asc
```

ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.deb.asc
```

Ensuite, consultez Vérification de la signature du package Mountpoint pour Amazon S3.

4. Installez le package à l'aide de la commande suivante :

```
sudo apt-get install ./mount-s3.deb
```

5. Vérifiez que Mountpoint pour Amazon S3 est correctement installé en exécutant la commande suivante :

```
mount-s3 --version
```

Vous devez voir des résultats similaires à ce qui suit :

```
mount-s3 1.3.1
```

Autres distributions Linux

1. Consultez la documentation de votre système d'exploitation pour installer les packages FUSE et `libfuse2`, qui sont obligatoires.
2. Copiez l'URL de téléchargement pour votre architecture.

   x86_64:

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz
```

   ARM64 (Graviton):

```
https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz
```

3. Téléchargez le package Mountpoint pour Amazon S3. Remplacez *`download-link`* par l'URL de téléchargement appropriée indiquée à l'étape précédente.

```
wget download-link
```

4. (Facultatif) Vérifiez l'authenticité et l'intégrité du fichier téléchargé. Tout d'abord, copiez l'URL de signature pour votre architecture.

   x86_64:

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.tar.gz.asc
   ```

   ARM64 (Graviton):

   ```
   https://s3.amazonaws.com/mountpoint-s3-release/latest/arm64/mount-s3.tar.gz.asc
   ```

   Ensuite, consultez Vérification de la signature du package Mountpoint pour Amazon S3.

5. Installez le package à l'aide de la commande suivante :

   ```
   sudo mkdir -p /opt/aws/mountpoint-s3 && sudo tar -C /opt/aws/mountpoint-s3 -xzf ./
   mount-s3.tar.gz
   ```

6. Ajoutez le fichier binaire `mount-s3` à votre variable d'environnement `PATH`. Dans votre fichier `$HOME/.profile`, ajoutez la ligne suivante :

   ```
   export PATH=$PATH:/opt/aws/mountpoint-s3/bin
   ```

   Enregistrez le fichier `.profile` et exécutez la commande suivante :

   ```
   source $HOME/.profile
   ```

7. Vérifiez que Mountpoint pour Amazon S3 est correctement installé en exécutant la commande suivante :

   ```
   mount-s3 --version
   ```

   Vous devez voir des résultats similaires à ce qui suit :

   ```
   mount-s3 1.3.1
   ```

Vérification de la signature du package Mountpoint pour Amazon S3

1. Installez GnuPG (commande gpg). Il est nécessaire de vérifier l'authenticité et l'intégrité d'un package Mountpoint pour Amazon S3 téléchargé. GnuPGest installé par défaut sur Amazon Linux Amazon Machine Images (AMIs). Après avoir installé GnuPG, passez à l'étape 2.
2. Téléchargez la clé publique Mountpoint en exécutant la commande suivante :

   ```
   wget https://s3.amazonaws.com/mountpoint-s3-release/public_keys/KEYS
   ```

3. Importez la clé publique Mountpoint dans votre trousseau de clés en exécutant la commande suivante :

   ```
   gpg --import KEYS
   ```

4. Vérifiez l'empreinte digitale de la clé publique Mountpoint en exécutant la commande suivante :

   ```
   gpg --fingerprint mountpoint-s3@amazon.com
   ```

   Confirmez que la chaîne d'empreinte digitale affichée correspond à ce qui suit :

   ```
   673F E406 1506 BB46 9A0E  F857 BE39 7A52 B086 DA5A
   ```

   Si la chaîne d'empreinte digitale ne correspond pas, ne terminez pas l'installation de Mountpoint et contactez AWS Support.

5. Téléchargez le fichier de signature de package. Remplacez *signature-link* par le lien de signature appropriée provenant des sections précédentes.

   ```
   wget signature-link
   ```

6. Vérifiez la signature du package téléchargé en exécutant la commande suivante. Remplacez *signature-filename* par le nom de fichier provenant de l'étape précédente.

   ```
   gpg --verify signature-filename
   ```

   Par exemple, dans les distributions basées sur RPM, y compris Amazon Linux, saisissez la commande suivante :

```
gpg --verify mount-s3.rpm.asc
```

7. La sortie doit inclure l'expression `Good signature`. Si la sortie inclut l'expression `BAD signature`, téléchargez à nouveau le fichier du package Mountpoint et répétez ces étapes. Si le problème persiste, ne terminez pas l'installation de Mountpoint et contactez AWS Support.

   La sortie peut inclure un avertissement concernant une signature approuvée. Cela n'indique pas qu'il y a un problème. Cela signifie simplement que vous n'avez pas vérifié de manière indépendante la clé publique Mountpoint.

Configuration et utilisation de Mountpoint

Pour utiliser Mountpoint pour Amazon S3, votre hôte a besoin AWS d'informations d'identification valides permettant d'accéder au ou aux compartiments Amazon S3 que vous souhaitez monter. Pour connaître les différentes méthodes d'authentification, consultez les informations d'identification AWS de Mountpoint sur GitHub.

Par exemple, vous pouvez créer un nouvel utilisateur AWS Identity and Access Management (IAM) et un nouveau rôle à cette fin. Assurez-vous que ce rôle a accès au ou aux compartiments que vous souhaitez monter. Vous pouvez transmettre le rôle IAM à votre EC2 instance Amazon à l'aide d'un profil d'instance.

Rubriques

- Utilisation de Mountpoint pour Amazon S3
- Configuration de la mise en cache dans Mountpoint

Utilisation de Mountpoint pour Amazon S3

Utilisez Mountpoint pour Amazon S3 pour effectuer les opérations suivantes :

1. Montez vos compartiments Amazon S3.

   a. Vous pouvez monter des buckets Amazon S3 manuellement à l'aide de la `mount-s3` commande.

Dans l'exemple suivant, remplacez *amzn-s3-demo-bucket* par le nom de votre compartiment S3 et remplacez *~/mnt* par le répertoire situé sur votre hôte, où vous souhaitez que votre compartiment S3 soit monté.

```
mkdir ~/mnt
mount-s3 amzn-s3-demo-bucket ~/mnt
```

Comme le client Mountpoint s'exécute en arrière-plan par défaut, le *~/mnt* répertoire vous donne désormais accès aux objets de votre compartiment Amazon S3.

b. Vous pouvez également configurer le montage automatique des buckets Amazon S3 lorsqu'une instance démarre ou redémarre.

Pour les EC2 instances Amazon existantes ou en cours d'exécution, recherchez le `fstab` fichier dans le `/etc/fstab` répertoire de votre système Linux. Ajoutez ensuite une ligne à votre `fstab` fichier. Par exemple, pour effectuer un montage *amzn-s3-demo-bucket* en utilisant le préfixe du chemin `example-prefix/` de votre système`/mnt/mountpoint`, consultez ce qui suit. Pour utiliser l'exemple suivant, remplacez les *user input placeholders* par vos propres informations.

```
s3://amzn-s3-demo-bucket/example-prefix/ /mnt/mountpoint mount-s3
 _netdev,nosuid,nodev,nofail,rw 0 0
```

Consultez le tableau suivant pour une explication des options utilisées dans l'exemple.

Option	Description
`_netdev`	Spécifie que le système de fichiers a besoin d'un réseau pour être monté.
`nosuid`	Spécifie que le système de fichiers ne peut pas contenir de fichiers d'ID utilisateur définis.
`nodev`	Spécifie que le système de fichiers ne peut pas contenir de périphériques spéciaux.

Option	Description
`nofail`	Spécifie que l'échec du montage du système de fichiers doit toujours permettre au système de démarrer.
`rw`	Spécifie que le point de montage est créé avec des autorisations de lecture et d'écriture. Vous pouvez également utiliser `ro` pour la lecture seule.

Pour les nouvelles EC2 instances Amazon, vous pouvez modifier les données utilisateur sur un EC2 modèle Amazon et configurer le `fstab` fichier comme suit. Pour utiliser l'exemple suivant, remplacez les *`user input placeholders`* par vos propres informations.

```
#!/bin/bash -e
MP_RPM=$(mktemp --suffix=.rpm)
curl https://s3.amazonaws.com/mountpoint-s3-release/latest/x86_64/mount-s3.rpm
 > $MP_RPM
yum install -y $MP_RPM
rm $MP_RPM

MNT_PATH=/mnt/mountpoint
echo "s3://amzn-s3-demo-bucket/ ${MNT_PATH} mount-s3
 _netdev,nosuid,nodev,rw,allow-other,nofail" >> /etc/fstab
mkdir $MNT_PATH

systemctl daemon-reload
mount -a
```

2. Accédez aux objets de votre compartiment Amazon S3 via Mountpoint.

   Après avoir monté votre compartiment localement, vous pouvez utiliser les commandes Linux courantes, telles que `cat` et `ls`, pour manipuler vos objets S3. Mountpoint pour Amazon S3 interprète les clés de votre compartiment Amazon S3 comme des chemins de système de fichiers en les divisant par une barre oblique (). `/` Par exemple, si vous avez la clé d'objet `Data/2023-01-01.csv` dans votre compartiment, vous aurez un répertoire nommé `Data`dans votre système de fichiers Mountpoint, avec un fichier nommé `2023-01-01.csv` à l'intérieur.

Mountpoint pour Amazon S3, volontairement, n'implémente pas l'intégralité de la spécification standard POSIX pour les systèmes de fichiers. Mountpoint est optimisé pour les charges de travail qui nécessitent un accès haut débit en lecture et en écriture aux données stockées dans Amazon S3 via une interface de système de fichiers, mais qui ne dépendent pas des fonctionnalités du système de fichiers. Pour plus d'informations, consultez le comportement du système de fichiers de Mountpoint pour Amazon S3 sur GitHub. Les clients qui ont besoin d'une sémantique de système de fichiers plus riche devraient envisager d'autres services de AWS fichiers, tels qu'Amazon Elastic File System (Amazon EFS) ou Amazon. FSx

3. Démontez votre compartiment Amazon S3 à l'aide de la `umount` commande. Cette commande démonte votre compartiment S3 et quitte Mountpoint.

   Pour utiliser l'exemple de commande suivant, remplacez *~/mnt* par le répertoire situé sur votre hôte, où votre compartiment S3 est monté.

   ```
   umount ~/mnt
   ```

   > **Note**
   >
   > Pour obtenir la liste des options pour cette commande, exécutez `umount --help`.

Pour plus de détails sur la configuration de Mountpoint, consultez les sections Configuration du compartiment Amazon S3 et configuration du système de fichiers sur. GitHub

Configuration de la mise en cache dans Mountpoint

Mountpoint pour Amazon S3 prend en charge différents types de mise en cache des données. Pour accélérer les demandes de lecture répétées, vous pouvez activer l'une des options suivantes :

- Cache local : vous pouvez utiliser un cache local dans le stockage de votre EC2 instance Amazon ou dans un volume Amazon Elastic Block Store. Si vous lisez à plusieurs reprises les mêmes données à partir de la même instance de calcul et si vous disposez d'un espace inutilisé dans le stockage de votre instance locale pour le jeu de données lu à plusieurs reprises, vous devez activer un cache local.
- Cache partagé : vous pouvez utiliser un cache partagé sur S3 Express One Zone. Si vous lisez de petits objets à plusieurs reprises à partir de plusieurs instances de calcul ou si vous ne connaissez

pas la taille de votre jeu de données lu régulièrement et souhaitez bénéficier de l'élasticité de la taille du cache, vous devez activer le cache partagé. Une fois que vous avez activé cette option, Mountpoint conserve les objets d'une taille maximale d'un mégaoctet dans un compartiment de répertoire qui utilise S3 Express One Zone.

- Cache local et cache partagé combinés : si vous avez de l'espace inutilisé dans votre cache local, mais que vous souhaitez également un cache partagé entre plusieurs instances, vous pouvez activer à la fois un cache local et un cache partagé.

La mise en cache dans Mountpoint est idéale pour les cas d'utilisation où vous lisez à plusieurs reprises les mêmes données qui ne changent pas au cours des multiples lectures. Par exemple, vous pouvez utiliser la mise en cache avec des tâches d'entraînement de machine learning qui nécessitent de lire plusieurs fois un jeu de données d'entraînement pour améliorer la précision du modèle.

Pour plus d'informations sur la configuration de la mise en cache dans Mountpoint, consultez les exemples suivants.

Rubriques

- Cache local
- Cache partagé
- Cache local et cache partagé combinés

Cache local

Vous pouvez activer un cache local à l'aide de l'indicateur `--cache` *`CACHE_PATH`*. Dans l'exemple suivant, remplacez *`CACHE_PATH`* par le chemin d'accès au répertoire dans lequel vous souhaitez mettre en cache les données. Remplacez-le *`amzn-s3-demo-bucket`* par le nom de votre compartiment Amazon S3, puis *`~/mnt`* par le répertoire sur votre hôte dans lequel vous souhaitez que votre compartiment S3 soit monté.

```
mkdir ~/mnt
mount-s3 --cache CACHE_PATH amzn-s3-demo-bucket ~/mnt
```

Lorsque vous optez pour la mise en cache locale lors du montage d'un compartiment Amazon S3, Mountpoint crée un sous-répertoire vide à l'emplacement de cache configuré, si ce sous-répertoire n'existe pas déjà. Lorsque vous montez un compartiment pour la première fois et que vous le démontez, Mountpoint supprime le contenu du cache local.

> **Important**
>
> Si vous activez la mise en cache locale, Mountpoint conservera le contenu de l'objet non chiffré de votre compartiment Amazon S3 monté à l'emplacement de cache local indiqué lors du montage. Afin de protéger vos données, vous devez restreindre l'accès à l'emplacement du cache de données en utilisant les mécanismes de contrôle d'accès du système de fichiers.

Cache partagé

Si vous lisez à plusieurs reprises de petits objets (jusqu'à 1 Mo) à partir de plusieurs instances de calcul ou si la taille du jeu de données que vous lisez à plusieurs reprises dépasse souvent la taille du cache local, vous devez utiliser un cache partagé dans S3 Express One Zone. Lorsque vous lisez les mêmes données à plusieurs reprises à partir de plusieurs instances, cela améliore la latence en évitant les demandes redondantes adressées à votre compartiment Amazon S3 monté.

Une fois que vous avez activé le cache partagé, vous payez les données mises en cache dans le compartiment de répertoire de S3 Express One Zone. Vous payez également les demandes effectuées sur vos données dans le compartiment de répertoire de S3 Express One Zone. Pour plus d'informations, consultez Tarification Amazon S3. Mountpoint ne supprime jamais les objets mis en cache à partir des compartiments de répertoire. Pour gérer les coûts de stockage, définissez une politique de cycle de vie pour votre compartiment de répertoire afin qu'Amazon S3 fasse expirer les données mises en cache dans S3 Express One Zone après une période que vous spécifiez. Pour plus d'informations, consultez Configuration de la mise en cache de Mountpoint pour Amazon S3 (langue française non garantie) sur GitHub.

Pour activer la mise en cache dans S3 Express One Zone lorsque vous montez un compartiment Amazon S3 sur votre instance de calcul, utilisez l'`--cache-xz`indicateur et spécifiez un compartiment de répertoire comme emplacement de cache. Dans l'exemple suivant, remplacez le*`user input placeholders`*.

```
mount-s3 amzn-s3-demo-bucket ~/mnt --cache-xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

Cache local et cache partagé combinés

Si vous avez de l'espace inutilisé dans votre cache local, mais que vous souhaitez également un cache partagé entre plusieurs instances, vous pouvez activer à la fois un cache local et un cache partagé. Avec cette configuration de mise en cache, vous pouvez éviter les demandes de lecture redondantes provenant de la même instance vers le cache partagé dans le compartiment

de répertoire lorsque les données requises sont mises en cache dans le stockage local. Cela peut réduire les coûts des demandes et améliorer les performances.

Pour activer à la fois un cache local et un cache partagé lorsque vous montez un compartiment Amazon S3, vous devez spécifier les deux emplacements de cache à l'aide `--cache-xz` des indicateurs `--cache` et. Pour utiliser l'exemple suivant pour activer à la fois un cache local et un cache partagé, remplacez le*user input placeholders*.

```
mount -s3 amzn-s3-demo-bucket ~/mnt --cache /path/to/mountpoint/cache --cache -xz amzn-s3-demo-bucket--usw2-az1--x-s3
```

Pour plus d'informations, consultez Configuration de la mise en cache de Mountpoint pour Amazon S3 (langue française non garantie) sur GitHub.

> **Important**
>
> Si vous activez la mise en cache partagée, Mountpoint copiera le contenu de l'objet depuis votre compartiment Amazon S3 monté vers le compartiment de répertoire S3 que vous fournissez comme emplacement de cache partagé, le rendant ainsi accessible à tout appelant ayant accès au compartiment d'annuaire S3. Pour protéger vos données mises en cache, conformez-vous aux Bonnes pratiques de sécurité pour Amazon S3 afin de vous assurer que vos compartiments utilisent les politiques appropriées et qu'ils ne sont pas accessibles publiquement. Utilisez un compartiment de répertoire dédié à la mise en cache partagée de Mountpoint et n'accordez l'accès qu'aux clients Mountpoint.

Dépannage de Mountpoint

Mountpoint pour Amazon S3 est soutenu par. Support Si vous avez besoin d'aide, contactez le Centre de AWS Support.

Vous pouvez également passer en revue et soumettre des problèmes Mountpoint sur GitHub.

Si vous découvrez un problème de sécurité potentiel dans ce projet, nous vous demandons de le signaler à AWS Security via notre page de signalement des vulnérabilités. Ne créez pas de problème GitHub public.

Si votre application se comporte de manière inattendue avec Mountpoint, vous pouvez consulter les informations de votre journal pour diagnostiquer le problème.

Journalisation

Par défaut, Mountpoint émet des informations de journal de haute gravité dans syslog.

Pour consulter les journaux dans la plupart des distributions Linux modernes, y compris Amazon Linux, exécutez la commande `journald` suivante :

```
journalctl -e SYSLOG_IDENTIFIER=mount-s3
```

Sur les autres systèmes Linux, les entrées `syslog` sont probablement écrites dans un fichier tel que `/var/log/syslog`.

Vous pouvez utiliser ces journaux pour dépanner votre application. Par exemple, si votre application tente de remplacer un fichier existant, l'opération échoue et vous verrez une ligne similaire à la suivante dans le journal :

```
[WARN] open{req=12 ino=2}: mountpoint_s3::fuse: open failed: inode error: inode 2 (full
 key "README.md") is not writable
```

Pour plus d'informations, consultez Journalisation (langue française non garantie) de Mountpoint pour Amazon S3 sur GitHub.

Utilisation du navigateur de stockage pour Amazon S3

Le navigateur de stockage pour S3 est un composant open source que vous pouvez ajouter à votre application web afin de fournir à vos utilisateurs finaux une interface graphique simple pour les données stockées dans Amazon S3. Avec le navigateur de stockage pour S3, vous pouvez fournir aux utilisateurs finaux autorisés un accès leur permettant de parcourir, télécharger, charger, copier et supprimer des données dans S3 directement à partir de vos propres applications.

Le navigateur de stockage pour S3 prend en charge les opérations suivantes pour les fichiers : `LIST`, `GET`, `PUT`, `COPY`, `UPLOAD` et `DELETE`. Pour permettre un transfert de données à haut débit, le navigateur de stockage pour S3 affiche uniquement les données auxquelles vos utilisateurs finaux peuvent accéder et optimise les demandes de chargement. Le navigateur de stockage optimise également les performances pour accélérer les temps de chargement, calcule les sommes de contrôle des données chargées par vos utilisateurs finaux et accepte les objets après avoir confirmé que l'intégrité de vos données a été préservée (en transit) sur l'Internet public. Vous pouvez contrôler l'accès à vos données en fonction de l'identité de votre utilisateur final à l'aide AWS de services de

sécurité et d'identité ou de vos propres services gérés. Vous pouvez également personnaliser le navigateur de stockage pour qu'il corresponde au design et à l'image de marque de votre application existante.

Le navigateur de stockage pour S3 n'est disponible que pour les applications web et intranet sur le framework React. Vous pouvez utiliser le navigateur de stockage pour accéder aux objets Amazon S3 dans toutes les classes de stockage, sauf S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, le niveau Archive Access de S3 Intelligent-Tiering et le niveau Deep Archive Access de S3 Intelligent-Tiering.

Le navigateur de stockage pour S3 peut être utilisé avec vos applications web dans la bibliothèque AWS Amplify React. Pour plus d'informations sur le navigateur de stockage, consultez Navigateur de stockage pour S3.

Rubriques

- Utilisation du navigateur de stockage pour S3
- Installation du navigateur de stockage pour S3
- Configuration du navigateur de stockage pour S3
- Configuration du navigateur de stockage pour S3
- Résolution des problèmes liés au navigateur de stockage pour S3

Utilisation du navigateur de stockage pour S3

Dans Storage Browser for S3, un emplacement est un compartiment ou un préfixe S3 à usage général auquel vous accordez l'accès aux utilisateurs finaux à l'aide des autorisations d'accès S3, des politiques IAM ou de votre propre service d'autorisation géré. Une fois que vous avez autorisé vos utilisateurs finaux à accéder à un emplacement spécifique, ils peuvent utiliser toutes les données de cet emplacement.

L'interface utilisateur du navigateur de stockage pour S3 comporte quatre vues principales :

- Page d'accueil : la page d'accueil répertorie les emplacements S3 auxquels vos utilisateurs peuvent accéder, ainsi que vos autorisations pour chacun d'entre eux. Il s'agit de la vue initiale pour les utilisateurs qui montre les ressources S3 de niveau racine auxquelles vos utilisateurs finaux ont accès et les autorisations (READ/WRITE/READWRITE) pour chaque emplacement S3.
- Détails de l'emplacement : cette vue permet aux utilisateurs de parcourir les fichiers et les dossiers dans S3, et de charger ou de télécharger des fichiers. Notez que dans le navigateur de stockage

pour S3, les objets sont appelés fichiers, tandis que les préfixes et les compartiments sont appelés dossiers.

- Action de localisation : une fois qu'un utilisateur a choisi une action (telle que le chargement) dans le navigateur de stockage, une autre vue de l'emplacement du fichier s'ouvre.
- Points de suspension verticaux : l'icône représentant des points de suspension verticaux ouvre la liste déroulante des actions.

Lorsque vous utilisez le navigateur de stockage pour S3, tenez compte des restrictions suivantes :

- Les dossiers commençant ou se terminant par un point (.) ne sont pas pris en charge.
- Les autorisations d'accès S3 ne permettent pas l'octroi d'autorisations en écriture seule.
- Le navigateur de stockage pour S3 prend en charge l'opération `PUT` pour les fichiers d'une taille maximale de 160 Go.
- Le navigateur de stockage pour S3 ne prend en charge l'opération `COPY` que pour les fichiers d'une taille inférieure à 5 Go. Si la taille du fichier dépasse 5 Go, le navigateur de stockage ne répondra pas à la demande.

Installation du navigateur de stockage pour S3

Le moyen le plus rapide de démarrer avec Storage Browser est de cloner l'un des exemples de projets sur GitHub. Ces exemples de projets peuvent vous aider à déployer des applications Web prêtes pour la production pour Storage Browser avec des intégrations de AWS services prédéfinies AWS Identity and Access Management afin de connecter rapidement les utilisateurs finaux autorisés aux données de S3.

Pour plus d'informations, voir Démarrage rapide dans le centre de développement Amplify.

Installation du navigateur de stockage pour S3 à partir de GitHub

Vous pouvez également installer Storage Browser pour S3 à partir de la dernière version `aws-amplify/ui-react-storage` et des `aws-amplify` packages du `aws-amplify` GitHubréférentiel pour commencer à intégrer Storage Browser à votre application existante. Lorsque vous installez le navigateur de stockage pour S3, veillez à ajouter les dépendances suivantes à votre fichier `package.json` :

```
"dependencies": {
```

```
    "aws-amplify/ui-react-storage": "latest",
    "aws-amplify": "latest",
  }
```

Vous pouvez aussi ajouter les dépendances à l'aide du Gestionnaire de package de nœud :

```
npm i --save @aws-amplify/ui-react-storage aws-amplify
```

Configuration du navigateur de stockage pour S3

Pour connecter les utilisateurs finaux aux emplacements Amazon S3, vous devez d'abord configurer une méthode d'authentification et d'autorisation. Il existe trois méthodes pour configurer une méthode d'authentification et d'autorisation avec le navigateur de stockage :

- Méthode 1 : gérer l'accès aux données pour vos clients et partenaires tiers
- Méthode 2 : gestion de l'accès aux données pour vos principaux IAM pour votre compte AWS
- Méthode 3 : gestion de l'accès aux données à l'échelle

Méthode 1 : gérer l'accès aux données pour vos clients et partenaires tiers

Avec cette méthode, vous pouvez utiliser AWS Amplify Auth pour gérer le contrôle d'accès et la sécurité des fichiers. Cette méthode est idéale lorsque vous souhaitez connecter vos clients ou partenaires tiers aux données dans S3. Grâce à cette option, vos clients peuvent s'authentifier à l'aide de fournisseurs d'identité sociaux ou d'entreprise.

Vous fournissez des informations d'identification IAM à vos utilisateurs finaux et à des partenaires tiers à l'aide d' AWS Amplify Auth avec un compartiment S3 configuré pour utiliser Amplify Storage. AWS Amplify Auth repose sur Amazon Cognito, un service de gestion de l'identité et de l'accès des clients entièrement géré qui vous permet d'authentifier et d'autoriser les utilisateurs à partir d'un annuaire d'utilisateurs ou d'un annuaire d'entreprise intégré, ou auprès de fournisseurs d'identité de consommateurs. Le modèle d'autorisation Amplify définit les préfixes auxquels l'utilisateur authentifié actif peut accéder. Pour plus d'informations sur la configuration de l'autorisation pour AWS Amplify, consultez Configuration du stockage.

Pour initialiser le composant avec les méthodes d'authentification et de stockage Amplify, ajoutez l'extrait de code suivant à votre application web :

```
import {
```

```
  createAmplifyAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

import config from './amplify_outputs.json';

Amplify.configure(config);

export const { StorageBrowser } = createStorageBrowser({
  config: createAmplifyAuthAdapter(),
});
```

Méthode 2 : gestion de l'accès aux données pour vos principaux IAM pour votre compte AWS

Si vous souhaitez gérer l'accès pour vos principaux IAM ou Compte AWS directement, vous pouvez créer un rôle IAM autorisé à invoquer l'opération d'API GetDataAccessS3. Pour configurer cela, vous devez créer une instance S3 Access Grants afin de mapper les autorisations pour les compartiments à usage général et les préfixes S3 aux identités IAM spécifiées. Le composant Storage Browser (qui doit être appelé côté client après avoir obtenu les informations d'identification IAM) invoquera ensuite l'opération d'API ListCallerAccessGrantsS3 pour récupérer les autorisations disponibles auprès du demandeur d'identité et renseigner les emplacements dans le composant. Une fois que vous avez obtenu l'autorisation `s3:GetDataAccess`, ces informations d'identification sont ensuite utilisées par le composant Navigateur de stockage pour demander l'accès aux données à S3.

```
import {
  createManagedAuthAdapter,
  createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import "@aws-amplify/ui-react-storage/styles.css";

export const { StorageBrowser } = createStorageBrowser({
  config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
```

```
          expiration: new Date()
        },
      }
    },
    // AWS `region` and `accountId`
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
});
```

Méthode 3 : gestion de l'accès aux données à l'échelle

Si vous souhaitez associer une instance d'autorisations d'accès S3 à IAM Identity Center pour bénéficier d'une solution plus évolutive (par exemple, si vous souhaitez fournir l'accès aux données à l'ensemble de votre entreprise), vous pouvez demander des données à Amazon S3 au nom de l'utilisateur authentifié actuel. Par exemple, vous pouvez autoriser les groupes d'utilisateurs de votre annuaire d'entreprise à accéder à vos données dans S3. Cette approche vous permet de gérer de manière centralisée les autorisations d'octroi d'accès S3 pour vos utilisateurs et groupes, y compris celles hébergées par des fournisseurs externes tels que Microsoft Entra, Okta, etc.

Lorsque vous utilisez cette méthode, l'intégration à l'IAM Identity Center vous permet d'utiliser les annuaires d'utilisateurs existants. Un autre avantage de la propagation d'identité approuvée d'IAM Identity Center est que chaque événement de données AWS CloudTrail pour Amazon S3 contient une référence directe à l'identité de l'utilisateur final qui a accédé aux données S3.

Si votre application prend en charge la OAuth version 2.0 et que vos utilisateurs ont besoin d'accéder à des AWS services depuis ces applications, nous vous recommandons d'utiliser la propagation d'identité sécurisée. Grâce à la propagation sécurisée des identités, un utilisateur peut se connecter à une application, et cette application peut transmettre son identité dans toutes les demandes d'accès aux données des AWS services. Cette application interagit avec IAM Identity Center pour le compte de tous les utilisateurs authentifiés. Pour plus d'informations, consultez Utilisation de la propagation d'identité approuvée entre applications.

La propagation fiable des identités est une AWS IAM Identity Center fonctionnalité que les administrateurs de Connected Services AWS peuvent utiliser pour accorder et auditer l'accès aux données de service. L'accès à ces données est basé sur les attributs de l'utilisateur tels que les associations de groupes. La mise en place d'une propagation d'identité sécurisée nécessite

une collaboration entre les administrateurs de Connected Services AWS et les administrateurs d'IAM Identity Center. Pour plus d'informations, consultez la section Conditions préalables et considérations.

Configuration

Pour configurer l'authentification du navigateur de stockage dans le cadre de la propagation d'identité sécurisée à AWS Management Console l'aide de S3 Access Grants et d'IAM Identity Center, vos applications doivent demander des données à Amazon S3 au nom de l'utilisateur authentifié actuel. Grâce à cette approche, vous pouvez donner aux utilisateurs ou aux groupes d'utilisateurs de votre annuaire d'entreprise un accès direct à vos compartiments, préfixes ou objets S3. Votre application n'a donc pas besoin de mapper des utilisateurs à un principal IAM.

Le flux de travail suivant décrit les étapes de configuration du navigateur de stockage pour S3, à l'aide d'IAM Identity Center et des autorisations d'accès S3 :

Étapes	Description
1	Activation d'IAM Identity Center pour AWS Organizations
2	Configuration de la fédération AWS Identity and Access Management Identity Center
3	Ajout d'un émetteur de jetons approuvés dans la console AWS Identity and Access Management Identity Center L'émetteur de jetons approuvés représente votre fournisseur d'identité (IdP) externe au sein d'IAM Identity Center, ce qui lui permet de reconnaître les jetons d'identité des utilisateurs authentifiés de votre application.
4	Création d'un rôle IAM pour l'application `bootstrap` et le `identity bearer`
5	Création et configuration de votre application dans IAM Identity Center Cette application interagit avec IAM Identity Center pour le compte des utilisateurs authentifiés.

Étapes	Description
6	Ajout des autorisations d'accès S3 en tant qu'application approuvée pour la propagation des identités Cette étape connecte votre application aux autorisations d'accès S3, afin qu'elle puisse envoyer des demandes aux autorisations d'accès S3 au nom des utilisateurs authentifiés.
7	Création d'une autorisation pour un utilisateur ou un groupe d'utilisateurs Cette étape synchronise les utilisateurs depuis AWS Identity and Access Management Identity Center avec le système de gestion des identités interdomaines (SCIM). SCIM synchronise les identités de votre IAM Identity Center avec les identités de votre fournisseur d'identité (IdP).
8	Création du composant Navigateur de stockage pour S3

Activation d'IAM Identity Center pour AWS Organizations

Pour activer IAM Identity Center pour votre AWS Organizations, effectuez les opérations suivantes :

1. Connectez-vous au AWS Management Console, en utilisant l'une des méthodes suivantes :
    1. Nouvel utilisateur AWS (utilisateur root) : connectez-vous en tant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.
    2. Vous utilisez déjà AWS (informations d'identification IAM) : connectez-vous à l'aide de vos informations d'identification IAM avec des autorisations administratives.
2. Ouvrez la console IAM Identity Center.
3. Sous Activer IAM Identity Center, sélectionnez Activer.

> **Note**
>
> IAM Identity Center nécessite la configuration de. AWS Organizations Si vous n'avez pas créé d'organisation, vous pouvez choisir d'en AWS créer une pour vous. Choisissez Créer une AWS organisation pour terminer ce processus.

4. Choisissez Activer avec AWS Organizations.
5. Choisissez Continuer.
6. (Facultatif) Ajoutez les balises que vous souhaitez associer à l'instance de cette organisation.
7. (Facultatif) Configurez l'administration déléguée.

> **Note**
>
> Si vous utilisez un environnement à plusieurs comptes, nous vous recommandons de configurer l'administration déléguée. Grâce à l'administration déléguée, vous pouvez limiter le nombre de personnes ayant besoin d'accéder au compte de gestion dans AWS Organizations. Pour plus d'informations, consultez Administration déléguée.

8. Choisissez Enregistrer.

AWS Organizations envoie automatiquement un e-mail de vérification à l'adresse associée à votre compte de gestion. Il peut y avoir un délai avant la réception de l'e-mail de vérification. Assurez-vous de vérifier votre adresse e-mail dans les 24 heures, avant l'expiration de l'e-mail de vérification.

Configuration de la fédération AWS Identity and Access Management Identity Center

Pour utiliser le navigateur de stockage pour S3 avec les utilisateurs de l'annuaire d'entreprise, vous devez configurer IAM Identity Center pour qu'il utilise un fournisseur d'identité (IdP) externe. Vous pouvez utiliser le fournisseur d'identité de votre choix. Sachez toutefois que chaque fournisseur d'identité utilise des paramètres de configuration différents. Pour en savoir plus sur l'utilisation de différents fournisseurs d'identité externes, consultez les didacticiels sources d'IAM Identity Center.

> **Note**
>
> Assurez-vous d'enregistrer l'URL de l'émetteur et les attributs d'audience du fournisseur d'identité que vous avez configuré, car vous devrez vous y référer ultérieurement. Si vous ne disposez pas de l'accès ni des autorisations nécessaires pour configurer un fournisseur

d'identité externe, vous devrez peut-être contacter l'administrateur de ce fournisseur pour les obtenir.

Ajout d'un émetteur de jetons approuvés dans la console AWS Identity and Access Management Identity Center

L'émetteur de jetons approuvés représente votre fournisseur d'identité externe au sein d' AWS Identity and Access Management Identity Center, et reconnaît les jetons d'identité des utilisateurs authentifiés de votre application. Le propriétaire du compte de l'instance IAM Identity Center de votre ordinateur AWS Organizations doit effectuer ces étapes. Cela peut avoir lieu soit dans la console IAM Identity Center, soit par programmation.

Pour ajouter un émetteur de jetons de confiance dans la console AWS Identity and Access Management Identity Center, effectuez les opérations suivantes :

1. Ouvrez la console IAM Identity Center.
2. Sélectionnez Paramètres.
3. Choisissez l'onglet Authentification.
4. Accédez à la section Émetteurs de jetons approuvés et renseignez les informations suivantes :
    1. Sous URL de l'émetteur, entrez l'URL du fournisseur d'identité externe qui sert d'émetteur de jetons approuvés. Vous devrez peut-être contacter l'administrateur du fournisseur d'identité externe pour obtenir ces informations. Pour plus d'informations, consultez Utilisation d'applications avec un émetteur de jetons approuvés.
    2. Sous Nom de l'émetteur de jeton approuvé, entrez le nom de l'émetteur de jetons approuvés. Ce nom apparaît dans la liste des émetteurs de jetons approuvés que vous pouvez sélectionner à l'étape 8, lorsqu'une ressource d'application est configurée pour la propagation des identités.
5. Mettez à jour la section Mapper les attributs en fonction de l'attribut de votre application préférée. Notez que chaque attribut du fournisseur d'identité est mappé à un attribut d'IAM Identity Center. Par exemple, vous pouvez mapper l'attribut d'application `email` à l'attribut utilisateur IAM Identity Center `email`. Pour consulter la liste des attributs utilisateur autorisés dans IAM Identity Center, consultez le tableau figurant dans la section Mappages d'attributs pour le répertoire AWS Microsoft AD géré.

6. (Facultatif) Si vous souhaitez ajouter une balise de ressource, entrez la paire clé/valeur. Pour ajouter plusieurs balises de ressources, choisissez Ajouter une nouvelle balise afin de générer une nouvelle entrée, puis saisissez les paires clé/valeur.
7. Choisissez Créer un émetteur de jetons approuvés.
8. Une fois que vous avez créé l'émetteur de jetons approuvés, contactez l'administrateur de l'application pour lui communiquer le nom de l'émetteur de jetons approuvés, afin qu'il puisse confirmer que cet émetteur est visible dans la console appropriée.
9. Assurez-vous que l'administrateur de l'application sélectionne cet émetteur de jetons approuvés dans la console applicable pour permettre l'accès utilisateur à l'application à partir d'applications configurées pour la propagation d'identité approuvée.

Création d'un rôle IAM pour l'application **`bootstrap`** et le **`identity bearer`**

Pour que l'application `bootstrap` et les utilisateurs du `identity bearer` puissent interagir de manière appropriée, veillez à créer deux rôles IAM. Un rôle IAM est requis pour l'application `bootstrap`, et l'autre rôle IAM doit être utilisé pour le porteur d'identité ou pour les utilisateurs finaux qui accèdent à l'application web demandant l'accès via les autorisations d'accès S3. L'application `bootstrap` recevra le jeton émis par le fournisseur d'identité et invoquera l'API `CreateTokenWithIAM`, en échangeant ce jeton avec celui émis par Identity Center.

Créez un rôle IAM, comme `bootstrap-role`, avec les autorisations suivantes. L'exemple suivant de politique IAM donne les autorisations nécessaires pour que `bootstrap-role` effectue l'échange de jetons :

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Action": [
            "sso-oauth:CreateTokenWithIAM",
        ],
        "Resource": "arn:${Partition}:sso::${AccountId}:application/${InstanceId}/
${ApplicationId}",
        "Effect": "Allow"
    },
    {
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext"
        ],
```

```
        "Resource": "arn:aws:iam::${AccountId}:role/identity-bearer-role",
        "Effect": "Allow"
    }]
}
```

Créez ensuite un deuxième rôle IAM (comme `identity-bearer-role`), que le fournisseur d'identité utilisera pour générer les informations d'identification IAM. Les informations d'identification IAM renvoyées par le fournisseur d'identité à l'application web sont utilisées par le composant Navigateur de stockage pour S3 afin d'autoriser l'accès aux données S3 :

```
{
    "Action": [
        "s3:GetDataAccess",
        "s3:ListCallerAccessGrants",
    ],
    "Resource": "arn:${Partition}:s3:${Region}:${Account}:access-grants/default",
    "Effect": "Allow"
}
```

Ce rôle IAM (`identity-bearer-role`) doit utiliser une politique d'approbation avec l'instruction suivante :

```
{
   "Effect": "Allow",
   "Principal": {
      "AWS": "arn:${Partition}:iam::${Account}:role/${RoleNameWithPath}"
   },
   "Action": [
       "sts:AssumeRole",
       "sts:SetContext"
   ]
}
```

Création et configuration de votre application dans IAM Identity Center

> **Note**
>
> Avant de commencer, vérifiez que vous avez créé les rôles IAM requis à l'étape précédente. Vous devrez spécifier l'un de ces rôles IAM au cours de cette étape.

Pour créer et configurer une application gérée par le client dans AWS IAM Identity Center, effectuez les étapes suivantes :

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Gérée par le client.
4. Choisissez Add application (Ajouter une application).
5. Sur la page Sélectionner le type d'application, sous Préférence de configuration, choisissez J'ai une application que je souhaite configurer.
6. Sous Type d'application, choisissez OAuth2.0.
7. Choisissez Suivant. La page Spécifier l'application s'affiche.
8. Dans la section Nom et description de l'application, entrez un nom d'affichage pour l'application, tel que **`storage-browser-oauth`**.
9. Saisissez une Description. La description de l'application apparaît dans la console IAM Identity Center et dans les demandes d'API, mais pas dans le portail AWS d'accès.
10. Sous Procédé d'affectation des utilisateurs et des groupes, choisissez Ne pas exiger d'affectations. Cette option permet à tous les utilisateurs et groupes autorisés d'IAM Identity Center d'accéder à cette application.
11. Sous Portail d'accès AWS , entrez l'URL de l'application à laquelle les utilisateurs peuvent accéder.
12. (Facultatif) Si vous souhaitez ajouter une balise de ressource, entrez la paire clé/valeur. Pour ajouter plusieurs balises de ressources, choisissez Ajouter une nouvelle balise afin de générer une nouvelle entrée, puis saisissez les paires clé/valeur.
13. Choisissez Suivant. La page de spécification de l'authentification s'affiche.
14. Sous Authentification avec un émetteur de jetons approuvés, cochez la case pour sélectionner l'émetteur de jetons approuvés que vous avez créé précédemment.
15. Sous Configurer les émetteurs de jeton approuvé sélectionné, entrez la réclamation Aud. La réclamation Aud identifie l'audience du jeton web JSON, ou jeton JWT. Il s'agit du nom sous lequel l'émetteur de jetons approuvés identifie cette application.

> **Note**
>
> Vous devrez peut-être contacter l'administrateur du fournisseur d'identité externe pour obtenir ces informations.

16. Choisissez Suivant. La page de spécification des informations d'identification pour l'authentification s'affiche.
17. Sous Méthode de configuration, choisissez Saisir un ou plusieurs rôles IAM.
18. Sous Saisir les rôles IAM, ajoutez le rôle IAM ou l' Amazon Resource Name (ARN) du jeton porteur d'identité. Vous devez saisir le rôle IAM que vous avez créé à l'étape précédente pour l'application de fournisseur d'identité (par exemple, **`bootstrap-role`**).
19. Choisissez Suivant.
20. Sur la page Vérification et configuration, passez en revue les détails de la configuration de votre application. Si vous devez modifier des paramètres, choisissez Modifier pour la section que vous souhaitez modifier, puis apportez les modifications nécessaires.
21. Sélectionnez Envoyer. La page de détails de l'application que vous venez d'ajouter s'affiche.

Une fois que vous avez configuré vos applications, vos utilisateurs peuvent y accéder depuis leur portail AWS d'accès en fonction des ensembles d'autorisations que vous avez créés et de l'accès utilisateur que vous avez attribué.

Ajout des autorisations d'accès S3 en tant qu'application approuvée pour la propagation des identités

Après avoir configuré votre application gérée par le client, vous devez spécifier les autorisations d'accès S3 pour la propagation des identités. Les autorisations d'accès S3 fournissent des informations d'identification aux utilisateurs pour qu'ils puissent accéder aux données Amazon S3. Lorsque vous vous connectez à votre application gérée par le client, les autorisations d'accès S3 transmettent votre identité d'utilisateur à l'application approuvée.

Prérequis : assurez-vous d'avoir configuré les autorisations d'accès S3 (par exemple, en créant une instance d'autorisations d'accès S3 et en enregistrant un emplacement) avant de suivre ces étapes. Pour plus d'informations, consultez Bien démarrer avec les autorisations d'accès S3.

Pour ajouter des autorisations d'accès S3 à des fins de propagation d'identité à votre application gérée par le client, effectuez les opérations suivantes :

1. Ouvrez la console IAM Identity Center.
2. Choisissez Applications.
3. Choisissez l'onglet Gérée par le client.
4. Dans la liste des applications gérées par le client, sélectionnez l'application OAuth 2.0 pour laquelle vous souhaitez lancer des demandes d'accès. Il s'agit de l'application à laquelle vos utilisateurs se connecteront.

5. Sur la page Détails, sous Applications approuvées pour la propagation d'identité, choisissez Spécifier les applications approuvées.
6. Sous Type de configuration, sélectionnez Applications individuelles et spécifiez l'accès, puis choisissez Suivant.
7. Sur la page Sélectionner un service, choisissez Autorisations d'accès S3. Les autorisations d'accès S3 comprennent des applications que vous pouvez utiliser pour définir votre propre application web pour la propagation d'identité approuvée.
8. Choisissez Suivant. Vous sélectionnerez vos applications à l'étape suivante.
9. Sur la page Sélectionner les applications, choisissez Applications individuelles, cochez la case correspondant à chaque application pouvant recevoir des demandes d'accès, puis choisissez Suivant.
10. Sur la page Configuration d'accès, sous Méthode de configuration, sélectionnez l'une des options suivantes :

    - Sélectionnez l'accès pour chaque application : sélectionnez cette option pour configurer différents niveaux d'accès pour chaque application. Choisissez l'application pour laquelle vous souhaitez configurer le niveau d'accès, puis choisissez Modifier l'accès. Dans Niveau d'accès à appliquer, modifiez les niveaux d'accès selon vos besoins, puis sélectionnez Enregistrer les modifications.
    - Appliquer le même niveau d'accès à toutes les applications : sélectionnez cette option si vous n'avez pas besoin de configurer les niveaux d'accès pour chaque application.
11. Choisissez Suivant.
12. Sur la page Vérifier la configuration, passez en revue les choix que vous avez effectués.

    > **Note**
    >
    > Assurez-vous que l'autorisation `s3:access_grants:read_write` est accordée à vos utilisateurs. Cette autorisation permet à vos utilisateurs de récupérer les informations d'identification leur permettant d'accéder à Amazon S3. Assurez-vous d'utiliser la politique IAM que vous avez créée précédemment, ou les autorisations d'accès S3, pour limiter l'accès aux opérations d'écriture.

13. Pour apporter des modifications, choisissez Modifier pour la section de configuration à laquelle vous voulez apporter des modifications. Effectuez les modifications nécessaires, puis sélectionnez Enregistrer les modifications.

14. Choisissez Applications approuvées pour ajouter l'application sécurisée pour la propagation d'identité.

Création d'une autorisation pour un utilisateur ou un groupe d'utilisateurs

Au cours de cette étape, vous utiliserez IAM Identity Center pour provisionner vos utilisateurs. Vous pouvez utiliser SCIM pour le provisionnement automatique ou manuel des utilisateurs et des groupes. SCIM synchronise les identités de votre IAM Identity Center avec les identités de votre fournisseur d'identité (IdP). Cela inclut le provisionnement, les mises à jour et le déprovisionnement des utilisateurs entre votre fournisseur d'identité et IAM Identity Center.

> **Note**
>
> Cette étape est nécessaire, car lorsque les autorisations d'accès S3 sont utilisées avec IAM Identity Center, les utilisateurs locaux d'IAM Identity Center ne sont pas utilisés. Au lieu de cela, les utilisateurs doivent être synchronisés depuis le fournisseur d'identité avec IAM Identity Center.

Pour synchroniser les utilisateurs du fournisseur d'identité avec IAM Identity Center, effectuez les opérations suivantes :

1. Activez le provisionnement automatique.
2. Générez un jeton d'accès.

Pour obtenir des exemples de configuration du fournisseur d'identité avec IAM Identity Center pour votre cas d'utilisation spécifique, consultez les didacticiels sur les sources d'identité d'IAM Identity Center.

Création du composant Navigateur de stockage pour S3

Après avoir configuré une instance IAM Identity Center et après avoir créé des autorisations dans les autorisations d'accès S3, ouvrez l'application React. Dans l'application React, utilisez `createManagedAuthAdapter` pour configurer les règles d'autorisation. Vous devez indiquer un fournisseur d'informations d'identification pour renvoyer les informations d'identification que vous avez obtenues auprès d'IAM Identity Center. Vous pouvez ensuite appeler `createStorageBrowser` pour initialiser le composant Navigateur de stockage pour S3 :

```
import {
    createManagedAuthAdapter,
    createStorageBrowser,
} from '@aws-amplify/ui-react-storage/browser';
import '@aws-amplify/ui-react-storage/styles.css';

export const { StorageBrowser } = createStorageBrowser({
   config: createManagedAuthAdapter({
    credentialsProvider: async (options?: { forceRefresh?: boolean }) => {
      // return your credentials object
      return {
        credentials: {
          accessKeyId: 'my-access-key-id',
          secretAccessKey: 'my-secret-access-key',
          sessionToken: 'my-session-token',
          expiration: new Date(),
        },
      }
    },
    // AWS `region` and `accountId` of the S3 Access Grants Instance.
    region: '',
    accountId: '',
    // call `onAuthStateChange` when end user auth state changes
    // to clear sensitive data from the `StorageBrowser` state
    registerAuthListener: (onAuthStateChange) => {},
  })
});
```

Créez ensuite un mécanisme pour échanger les jetons Web JSON (JWTs) de votre application Web avec les informations d'identification IAM d'IAM Identity Center. Pour plus d'informations sur l'échange de jetons JWT, consultez les ressources suivantes :

- Article How to develop a user-facing data application with IAM Identity Center and S3 Access Grants dans le blog AWS Storage
- Article Scaling data access with S3 Access Grants dans le blog AWS Storage
- S3 Access Grants workshop dans la documentation AWS Workshop Studio
- Atelier S3 Access Grants sur GitHub

Configurez ensuite un point de terminaison d'API pour gérer les demandes d'extraction d'informations d'identification. Pour valider l'échange de jetons web JSON (JWT), effectuez les opérations suivantes :

1. Récupérez le jeton web JSON à partir de l'en-tête d'autorisation des demandes entrantes.
2. Validez le jeton à l'aide des clés publiques de l'URL du jeu JWKS (JSON Web Key Set) spécifié.
3. Vérifiez les déclarations relatives à l'expiration, à l'émetteur, au sujet et à l'audience du jeton.

Pour échanger le jeton Web JSON du fournisseur d'identité avec les informations d'identification AWS IAM, effectuez les opérations suivantes :

> **Tip**
>
> Évitez de consigner des informations sensibles. Nous vous recommandons d'utiliser des contrôles de gestion des erreurs pour les autorisations manquantes, les jetons ayant expiré et les autres exceptions. Pour plus d'informations, consultez l'article Implémentation des modèles de gestion des AWS Lambda erreurs sur le blog AWS Compute.

1. Vérifiez que les paramètres Autorisation et Portée requis sont fournis dans la demande.
2. Utilisez l'API CreateTokenWithIAM pour échanger le jeton web JSON contre un jeton IAM Identity Center.

   > **Note**
   >
   > Une fois que le jeton Web JSON du fournisseur d'identité a été utilisé, il ne peut pas être réutilisé. Un nouveau jeton devra être utilisé pour l'échange avec IAM Identity Center.

3. Utilisez l'opération AssumeRoleAPI pour assumer un rôle transitoire à l'aide du jeton IAM Identity Center. Assurez-vous d'utiliser le rôle du porteur d'identité, également connu sous le nom de rôle porteur du contexte d'identité (par exemple, **`identity-bearer-role`**), pour demander les informations d'identification.
4. Renvoyez les informations d'identification IAM à l'application web.

> **Note**
>
> Assurez-vous d'avoir mis en place un mécanisme de journalisation approprié. Les réponses sont renvoyées dans un format JSON standardisé avec un code d'état HTTP approprié.

Configuration du navigateur de stockage pour S3

Pour permettre au navigateur de stockage pour S3 d'accéder aux compartiments S3, le composant Navigateur de stockage envoie les appels d'API REST à Amazon S3. Par défaut, le partage des ressources cross-origin (CORS) n'est pas activé au niveau des compartiments S3. Par conséquent, vous devez activer CORS pour chaque compartiment S3 à partir duquel le navigateur de stockage accède aux données.

Par exemple, pour activer CORS au niveau d'un compartiment S3, vous pouvez mettre à jour votre politique CORS comme suit :

```
[
    {
        "ID": "S3CORSRuleId1",
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "GET",
            "HEAD",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": [
            "last-modified",
            "content-type",
            "content-length",
            "etag",
            "x-amz-version-id",
```

```
            "x-amz-request-id",
            "x-amz-id-2",
            "x-amz-cf-id",
            "x-amz-storage-class",
            "date",
            "access-control-expose-headers"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

Résolution des problèmes liés au navigateur de stockage pour S3

Si vous rencontrez des problèmes avec le navigateur de stockage pour S3, reportez-vous aux conseils suivants de résolution des problèmes :

- N'essayez pas d'utiliser le même jeton (`idToken` ou `accessToken`) pour plusieurs demandes. Les jetons ne peuvent pas être réutilisés. Cela entraîne l'échec de la demande.
- Assurez-vous que les informations d'identification IAM que vous fournissez au composant Navigateur de stockage incluent les autorisations permettant d'invoquer l'opération `s3:GetDataAccess`. Dans le cas contraire, les utilisateurs ne parviendront pas à accéder à vos données.

Vous pouvez également consulter les ressources suivantes :

- Storage Browser pour S3 est soutenu par le AWS Support. Si vous avez besoin d'aide, contactez AWS Support Center.
- Si vous rencontrez des problèmes avec Storage Browser pour S3 ou si vous souhaitez envoyer des commentaires, rendez-vous sur la page Amplify GitHub .
- Si vous découvrez un problème de sécurité potentiel dans ce projet, vous pouvez le signaler à AWS Security via la page de signalement des vulnérabilités AWS.

Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration est une fonctionnalité au niveau du bucket qui permet des transferts rapides, faciles et sécurisés de fichiers sur de longues distances entre votre client et un

bucket S3 à usage général. L'accélération des transferts est conçue pour optimiser les vitesses de transfert depuis le monde entier vers des compartiments S3 à usage général. Transfer Acceleration tire parti des emplacements périphériques répartis dans le monde entier sur Amazon CloudFront. Lorsque les données arrivent dans un emplacement périphérique, elles sont transférées vers Amazon S3 sur un chemin de réseau optimisé.

Lorsque vous utilisez Transfer Acceleration, des frais supplémentaires de transfert de données peuvent s'appliquer. Pour plus d'informations sur la tarification, consultez Tarification Amazon S3.

Pourquoi utiliser Transfer Acceleration ?

Vous souhaiterez peut-être utiliser Transfer Acceleration sur un bucket à usage général pour différentes raisons :

- Vos clients téléchargent des données du monde entier vers un bucket à usage général centralisé.
- Vous transférez régulièrement de plusieurs gigaoctets à plusieurs téraoctets de données d'un continent à l'autre.
- Vous ne pouvez pas utiliser toute la bande passante disponible sur Internet lors du chargement vers Amazon S3.

Pour plus d'informations sur les circonstances dans lesquelles utiliser l'accélération des transferts, consultez Amazon S3 FAQs.

Conditions d'utilisation de Transfer Acceleration

Les conditions suivantes sont requises pour utiliser Transfer Acceleration sur un compartiment S3 :

- Transfer Acceleration n'est prise en charge que sur les demandes de type hébergement virtuel. Pour plus d'informations sur les demandes de style hébergement virtuel, consultez Demandes à l'aide de l'API REST dans la Référence d'API Amazon S3.
- Le nom du compartiment utilisé pour Transfer Acceleration doit être conforme aux règles DNS et ne doit pas inclure de points (« . »).
- Transfer Acceleration doit être activée sur le compartiment. Pour plus d'informations, consultez Activation et utilisation de S3 Transfer Acceleration.

  Une fois que vous activez Transfer Acceleration sur un compartiment, 20 minutes peuvent être nécessaires avant l'augmentation de la vitesse du transfert des données vers le compartiment.

> **Note**
>
> Transfer Acceleration est actuellement prise en charge pour les compartiments situés dans les régions suivantes :
>
> - Asie-Pacifique (Tokyo) (ap-northeast-1)
> - Asie-Pacifique (Séoul) (ap-northeast-2)
> - Asie-Pacifique (Mumbai) (ap-south-1)
> - Asie-Pacifique (Singapour) (ap-southeast-1)
> - Asie-Pacifique (Sydney) (ap-southeast-2)
> - Canada (Centre) (ca-central-1)
> - Europe (Francfort) (eu-central-1)
> - Europe (Irlande) (eu-west-1)
> - Europe (Londres) (eu-west-2)
> - Europe (Paris) (eu-west-3)
> - Amérique du Sud (São Paulo) (sa-east-1)
> - USA Est (Virginie du Nord) (us-east-1)
> - USA Est (Ohio) (us-east-2)
> - USA Ouest (Californie du Nord) (us-west-1)
> - USA Ouest (Oregon) (us-west-2)

- Pour accéder au compartiment activé pour Transfer Acceleration, vous devez utiliser le point de terminaison *`bucket-name`*`.s3-accelerate.amazonaws.com`. Vous pouvez également utiliser le point de terminaison *`bucket-name`*`.s3-accelerate.dualstack.amazonaws.com` à double pile pour vous connecter au bucket over IPv6 activé. Vous pouvez continuer à utiliser les points de terminaison habituels pour le transfert de données standard.
- Vous devez être le propriétaire du compartiment pour définir l'état de l'accélération du transfert. Le propriétaire du compartiment peut attribuer des autorisations à d'autres utilisateurs pour leur permettre de définir l'état de l'accélération dans un compartiment. L'autorisation `s3:PutAccelerateConfiguration` permet aux utilisateurs d'activer ou de désactiver Transfer Acceleration sur un compartiment. L'autorisation `s3:GetAccelerateConfiguration` permet aux utilisateurs de renvoyer l'état Transfer Acceleration d'un compartiment, qui est `Enabled` ou `Suspended`..

Les sections suivantes décrivent la manière de mettre en route et utiliser Amazon S3 Transfer Acceleration pour transférer des données.

Rubriques

- Mise en route d'Amazon S3 Transfer Acceleration
- Activation et utilisation de S3 Transfer Acceleration
- Utilisation de l'outil de comparaison de vitesse Amazon S3 Transfer Acceleration

Mise en route d'Amazon S3 Transfer Acceleration

Vous pouvez utiliser Amazon S3 Transfer Acceleration pour obtenir un transfert rapide, facile et sécurisé des fichiers sur des longues distances entre votre client et un compartiment S3. Transfer Acceleration utilise les emplacements périphériques répartis dans le monde entier sur Amazon CloudFront. Lorsque les données arrivent dans un emplacement périphérique, elles sont transférées vers Amazon S3 sur un chemin de réseau optimisé.

Pour commencer à utiliser Amazon S3 Transfer Acceleration, effectuez les étapes suivantes :

1. Activer Transfer Acceleration sur un compartiment

   Vous pouvez activer Transfer Acceleration sur un compartiment de l'une des manières suivantes :

   - Utilisez la console Amazon S3.
   - Utilisez l'PutBucketAccelerateConfigurationopération de l'API REST.
   - Utilise AWS CLI le sable AWS SDKs. Pour plus d'informations, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence des API Amazon S3.

   Pour de plus amples informations, veuillez consulter Activation et utilisation de S3 Transfer Acceleration.

   > **Note**
   >
   > Pour que votre bucket fonctionne avec l'accélération des transferts, le nom du bucket doit être conforme aux exigences de dénomination DNS et ne doit pas contenir de points (`.`).

2. Transférer des données vers et depuis le compartiment activé pour l'accélération

Utilisez l'un des noms de domaine de `s3-accelerate` point de terminaison suivants :

- Pour accéder à un compartiment activé pour l'accélération, veuillez utiliser *`bucket-name`*`.s3-accelerate.amazonaws.com`.
- Pour accéder à un bucket over activé pour l'accélération IPv6, utilisez. *`bucket-name`*`.s3-accelerate.dualstack.amazonaws.com`

  Les points de terminaison à double pile Amazon S3 prennent en charge les demandes adressées aux compartiments S3 sur et. IPv6 IPv4 Seul le point de terminaison double pile (« Dual-Stack ») Transfer Acceleration utilise le nom de point de terminaison de type hébergement virtuel. Pour plus d'informations, consultez Envoyer des demandes à Amazon S3 IPv6 dans la référence d'API Amazon S3 et Utilisation de points de terminaison à double pile d'Amazon S3 dans la référence d'API Amazon S3.

> **Note**
>
> Votre application de transfert de données doit utiliser l'un des deux types de points de terminaison suivants pour accéder au compartiment afin d'accélérer le transfert de données : `.s3-accelerate.amazonaws.com` ou `.s3-accelerate.dualstack.amazonaws.com` pour le point de terminaison à double pile. Si vous souhaitez utiliser le transfert de données standard, vous pouvez continuer à utiliser les points de terminaison habituels.

Vous pouvez rediriger votre PUT objet Amazon S3 et vos demandes d'`GET`objets vers le nom de domaine du `s3-accelerate` point de terminaison après avoir activé l'accélération des transferts. Supposons, par exemple, que vous utilisiez actuellement une application d'API REST PutObjectqui utilise le nom d'hôte indiqué *`amzn-s3-demo-bucket`*`.s3.us-east-1.amazonaws.com` dans la PUT demande. Pour accélérer le PUT, vous modifiez le nom d'hôte dans votre demande à *`amzn-s3-demo-bucket`*`.s3-accelerate.amazonaws.com`. Pour revenir à l'utilisation de la vitesse de chargement standard, remplacez le nom par *`amzn-s3-demo-bucket`*`.s3.us-east-1.amazonaws.com`.

Une fois que Transfer Acceleration est activé, il peut s'écouler jusqu'à 20 minutes pour que vous preniez conscience de l'avantage offert en termes de performance. Cependant, le point de terminaison d'accélération est disponible dès que vous activez Transfer Acceleration.

Vous pouvez utiliser le point de terminaison Accelerate dans AWS CLI AWS SDKs, et d'autres outils qui transfèrent des données vers et depuis Amazon S3. Si vous utilisez le AWS SDKs, certaines des langues prises en charge utilisent un indicateur de configuration du client de point de terminaison accéléré, de sorte que vous n'avez pas besoin de définir explicitement le point de terminaison sur lequel Transfer Acceleration est activé*bucket-name*.s3-accelerate.amazonaws.com. Pour obtenir des exemples d'utilisation d'un indicateur de configuration client du point de terminaison d'accélération, consultez la pageActivation et utilisation de S3 Transfer Acceleration.

Vous pouvez utiliser toutes les opérations Amazon S3 via les points de terminaison d'accélération de transfert, sauf pour les éléments suivants :

- ListBuckets
- CreateBucket
- DeleteBucket

De plus, Amazon S3 Transfer Acceleration ne prend pas en charge l'utilisation CopyObjectde copies entre régions.

Activation et utilisation de S3 Transfer Acceleration

Vous pouvez utiliser Amazon S3 Transfer Acceleration pour transférer des fichiers rapidement et en toute sécurité sur de longues distances entre votre client et un bucket S3 à usage général. Vous pouvez activer l'accélération des transferts à l'aide de la console S3, du AWS Command Line Interface (AWS CLI), de l'API ou du AWS SDKs.

Cette section propose des exemples d'activation d'Amazon S3 Transfer Acceleration sur un compartiment et d'utilisation du point de terminaison d'accélération pour le compartiment activé.

Pour en savoir plus sur les exigences de Transfer Acceleration, consultez Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.

Utilisation de la console S3

> **Note**
>
> Si vous souhaitez comparer les vitesses de chargement accéléré et non accéléré, ouvrez l'Outil de comparaison de la vitesse d'Amazon S3 Transfer Acceleration.

L'outil de comparaison de vitesse utilise le téléchargement en plusieurs parties pour transférer un fichier de votre navigateur vers différents navigateurs Régions AWS avec et sans accélération de transfert Amazon S3. Vous pouvez comparer la vitesse de téléchargement des téléchargements directs et transférer des téléchargements accélérés par Région.

Pour activer l'accélération des transferts pour un bucket S3 à usage général

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments à usage général, choisissez le nom du compartiment pour lequel vous souhaitez activer l'accélération des transferts.
4. Choisissez Propriétés.
5. Sous Transfer acceleration (Accélération du transfert), choisissez Edit (Modifier).
6. Sélectionnez Activer, puis Enregistrer les modifications.

Pour accéder à des transferts de données accélérés

1. Une fois qu'Amazon S3 active l'accélération du transfert pour votre compartiment, affichez l'onglet Propriétés pour le compartiment.
2. Sous Transfer acceleration (Accélération du transfert), Accelerated endpoint (Point de terminaison accéléré) affiche le point de terminaison Transfer Acceleration pour votre compartiment. Utilisez ce point de terminaison pour accéder à des transferts de données accélérés vers et depuis votre compartiment.

   Si vous interrompez Transfer Acceleration, le point de terminaison de l'accélération ne fonctionne plus.

À l'aide du AWS CLI

Voici des exemples de AWS CLI commandes utilisées pour l'accélération des transferts. Pour obtenir des instructions sur la configuration du AWS CLI, consultez la section Développement avec Amazon S3 AWS CLIà l'aide du document de référence sur les API Amazon S3.

Activation de Transfer Acceleration sur un compartiment

Utilisez la AWS CLI put-bucket-accelerate-configurationcommande pour activer ou suspendre l'accélération du transfert sur un bucket.

L'exemple suivant montre comment `Status=Enabled` activer l'accélération du transfert sur un bucket nommé*amzn-s3-demo-bucket*. Pour suspendre l'accélération du transfert, utilisez`Status=Suspended`.

Example

```
$ aws s3api put-bucket-accelerate-configuration --bucket amzn-s3-demo-bucket --
accelerate-configuration Status=Enabled
```

Utilisation de Transfer Acceleration

Vous pouvez diriger toutes les demandes `s3` et `s3api` AWS CLI commandes Amazon S3 effectuées par le point de terminaison accéléré :`s3-accelerate.amazonaws.com`. Pour ce faire, définissez la valeur `use_accelerate_endpoint` de configuration sur `true` dans un profil de votre AWS Config fichier. Transfer Acceleration doit être activé sur votre compartiment si vous souhaitez utiliser le point de terminaison d'accélération.

Toutes les demandes sont envoyées en utilisant le style virtuel de l'adressage de compartiment : *amzn-s3-demo-bucket*`.s3-accelerate.amazonaws.com`. Les requêtes `ListBuckets`, `CreateBucket` et `DeleteBucket` ne sont pas envoyées au point de terminaison d'accélération, car celui-ci ne prend pas en charge ces opérations.

Pour plus d'informations sur `use_accelerate_endpoint`, consultez Configuration S3 d'AWS CLI dans la Référence des commandes de l'AWS CLI .

L'exemple suivant définit `use_accelerate_endpoint` sur `true` dans le profil par défaut.

Example

```
$ aws configure set default.s3.use_accelerate_endpoint true
```

Si vous souhaitez utiliser le point de terminaison d'accélération pour certaines AWS CLI commandes mais pas pour d'autres, vous pouvez utiliser l'une des deux méthodes suivantes :

- Utilisez le point de terminaison d'accélération pour n'importe quelle `s3api` commande `s3` ou en réglant le `--endpoint-url` paramètre sur`https://s3-accelerate.amazonaws.com`.

- Configurez des profils distincts dans votre AWS Config dossier. Par exemple, vous pouvez créer un profil qui définit `use_accelerate_endpoint` sur `true` et un profil qui ne définit pas `use_accelerate_endpoint`. Lorsque vous exécutez une commande, spécifiez le profil que vous souhaitez utiliser en fonction de votre intention d'utiliser le point de terminaison d'accélération.

Chargement d'un objet dans un compartiment activé pour Transfer Acceleration

L'exemple suivant télécharge un fichier dans un compartiment nommé *amzn-s3-demo-bucket* qui a été activé pour l'accélération des transferts en utilisant le profil par défaut configuré pour utiliser le point de terminaison accéléré.

Example

```
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region
```

L'exemple suivant charge un fichier sur un compartiment activé pour Transfer Acceleration en utilisant le paramètre `--endpoint-url` pour spécifier le point de terminaison d'accélération.

Example

```
$ aws configure set s3.addressing_style virtual
$ aws s3 cp file.txt s3://amzn-s3-demo-bucket/key-name --region region --endpoint-url
 https://s3-accelerate.amazonaws.com
```

À l'aide du AWS SDKs

Voici des exemples d'utilisation de Transfer Acceleration pour charger des objets sur Amazon S3 à l'aide du AWS SDK. Certains langages pris en charge par le AWS SDK (par exemple, Java et.NET) utilisent un indicateur de configuration du client de point de terminaison accéléré, de sorte que vous n'avez pas besoin de définir explicitement le point de terminaison sur lequel Transfer Acceleration est activé. *bucket-name*`.s3-accelerate.amazonaws.com`

Java

Example

L'exemple suivant montre comment utiliser un point de terminaison d'accélération pour charger un objet sur Amazon S3. Cet exemple effectue les opérations suivantes :

- Crée un `AmazonS3Client` configuré pour utiliser les points de terminaison d'accélération. Tous les compartiments auxquels le client accède doivent avoir la fonction Transfer Acceleration activée.
- Active la fonction Transfer Acceleration sur un compartiment spécifié. Cette étape n'est nécessaire que si le compartiment que vous spécifiez ne possède pas déjà la fonction Transfer Acceleration activée.
- Vérifie que la fonction Transfer Acceleration est activée pour le compartiment spécifié.
- Charge un nouvel objet sur le compartiment spécifié à l'aide du point de terminaison d'accélération du compartiment.

Pour plus d'informations sur l'utilisation de Transfer Acceleration, consultez Mise en route d'Amazon S3 Transfer Acceleration. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketAccelerateConfiguration;
import com.amazonaws.services.s3.model.BucketAccelerateStatus;
import com.amazonaws.services.s3.model.GetBucketAccelerateConfigurationRequest;
import com.amazonaws.services.s3.model.SetBucketAccelerateConfigurationRequest;

public class TransferAcceleration {
    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";

        try {
            // Create an Amazon S3 client that is configured to use the accelerate
 endpoint.
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .enableAccelerateMode()
                    .build();
```

```
            // Enable Transfer Acceleration for the specified bucket.
            s3Client.setBucketAccelerateConfiguration(
                    new SetBucketAccelerateConfigurationRequest(bucketName,
                            new BucketAccelerateConfiguration(
                                    BucketAccelerateStatus.Enabled)));

            // Verify that transfer acceleration is enabled for the bucket.
            String accelerateStatus = s3Client.getBucketAccelerateConfiguration(
                    new GetBucketAccelerateConfigurationRequest(bucketName))
                    .getStatus();
            System.out.println("Bucket accelerate status: " + accelerateStatus);

            // Upload a new object using the accelerate endpoint.
            s3Client.putObject(bucketName, keyName, "Test object for transfer
 acceleration");
            System.out.println("Object \"" + keyName + "\" uploaded with transfer
 acceleration.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

L'exemple suivant montre comment utiliser le AWS SDK pour .NET pour activer l'accélération du transfert sur un bucket. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Premiers pas avec le kit AWS SDK pour .NET dans le Guide du développeur AWS SDK pour .NET .

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
```

```
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TransferAccelerationTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            EnableAccelerationAsync().Wait();
        }

        static async Task EnableAccelerationAsync()
        {
                try
                {
                    var putRequest = new PutBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName,
                        AccelerateConfiguration = new AccelerateConfiguration
                        {
                            Status = BucketAccelerateStatus.Enabled
                        }
                    };
                    await
 s3Client.PutBucketAccelerateConfigurationAsync(putRequest);

                    var getRequest = new GetBucketAccelerateConfigurationRequest
                    {
                        BucketName = bucketName
                    };
                    var response = await
 s3Client.GetBucketAccelerateConfigurationAsync(getRequest);

                    Console.WriteLine("Acceleration state = '{0}' ",
 response.Status);
                }
                catch (AmazonS3Exception amazonS3Exception)
```

```
                {
                    Console.WriteLine(
                        "Error occurred. Message:'{0}' when setting transfer
 acceleration",
                        amazonS3Exception.Message);
                }
            }
        }
    }
```

Lors du chargement d'un objet sur un compartiment pour lequel Transfer Acceleration est activé, vous spécifiez l'utilisation du point de terminaison d'accélération au moment de la création d'un client.

```
var client = new AmazonS3Client(new AmazonS3Config
            {
                RegionEndpoint = TestRegionEndpoint,
                UseAccelerateEndpoint = true
            }
```

JavaScript

Pour un exemple d'activation de l'accélération des transferts à l'aide de la PutBucketAccelerateConfigurationcommande AWS SDK pour JavaScript, voir la référence de l'AWS SDK pour JavaScript API.

Python (Bottes)

Pour un exemple d'activation de l'accélération des transferts à l'aide du SDK pour Python, consultez put_bucket_accelerate_configuration dans le manuel de référence de l'API du AWS SDK for Python (Boto3).

Other

Pour plus d'informations sur l'utilisation d'autres AWS SDKs, voir Exemples de code et bibliothèques.

Utilisation de l'API REST

Utilisez l'opération `PutBucketAccelerateConfiguration` de l'API REST pour accélérer la configuration sur un compartiment existant.

Pour plus d'informations, consultez PutBucketAccelerateConfiguration dans la Référence d'API Amazon Simple Storage Service.

Utilisation de l'outil de comparaison de vitesse Amazon S3 Transfer Acceleration

Vous pouvez utiliser l'outil de comparaison de vitesse Amazon S3 Transfer Acceleration pour comparer les vitesses de chargement accéléré et non accéléré dans les Régions Amazon S3. L'outil de comparaison de vitesse utilise les chargements partitionnés pour transférer un fichier à partir de votre navigateur vers différentes Régions Amazon S3 avec ou sans Transfer Acceleration.

Vous pouvez accéder à l'outil de comparaison de vitesse en utilisant l'une des méthodes suivantes :

- Copiez l'URL suivante dans la fenêtre de votre navigateur, en la *region* remplaçant par Région AWS celle que vous utilisez (par exemple`us-west-2`) et *amzn-s3-demo-bucket* par le nom du bucket que vous souhaitez évaluer :

  `https://s3-accelerate-speedtest.s3-accelerate.amazonaws.com/en/accelerate-speed-comparsion.html?region=`*region*`&origBucketName=`*amzn-s3-demo-bucket*

  Pour obtenir la liste des régions prises en charge par Amazon S3, consultez Points de terminaison et quotas Amazon S3 dans la Références générales AWS.
- Utilisez la console Amazon S3.

Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation

C'est en général le propriétaire du compartiment qui prend en charge l'ensemble des frais de stockage et de transfert de données Amazon S3 associés à son compartiment. Cependant, vous pouvez configurer un bucket à usage général pour qu'il soit un bucket Requester Pays. Lorsqu'un compartiment est de type Paiement par le demandeur, les frais associés à la demande et au téléchargement de données depuis le compartiment sont facturés au demandeur, et non plus propriétaire du compartiment. En revanche, les frais de stockage des données sont toujours facturés au propriétaire du compartiment.

En général, nous recommandons de configurer des compartiments de type Paiement par le demandeur lorsque vous souhaitez partager des données, sans supporter les frais d'accès des

autres utilisateurs. Par exemple, vous pouvez utiliser des compartiments Paiement par le demandeur lorsque vous proposez des jeux de données volumineux, tels que des répertoires de codes postaux, des données de référence, des informations géospatiales ou des données d'indexation de site Web.

> **Important**
>
> Si vous activez Requester Pays sur un compartiment à usage général, l'accès anonyme à ce compartiment n'est pas autorisé.

Vous devez authentifier toutes les demandes associées à vos compartiments de type Paiement par le demandeur. L'authentification des demandes permet à Amazon S3 d'identifier le demandeur et de lui facturer l'utilisation du compartiment de type Paiement par le demandeur.

Lorsque le demandeur assume un rôle AWS Identity and Access Management (IAM) avant de faire sa demande, le compte auquel appartient le rôle est débité pour la demande. Pour plus d'informations sur les rôles IAM, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

Une fois que vous configurez un compartiment de type Paiement par le demandeur, les demandeurs doivent attester qu'ils ont compris que les demandes et les téléchargements de données leur seront facturés. Pour ce faire, les demandeurs doivent soit inclure `x-amz-request-payer` comme en-tête dans leur demande d'API pour les requêtes DELETE, GET, HEAD, POST et PUT, soit ajouter le paramètre `RequestPayer` dans leur requête REST. Pour les demandes de CLI, les demandeurs peuvent utiliser le paramètre `--request-payer`.

Example — Utilisation du paiement par le demandeur lors de la suppression d'un objet

Pour utiliser l'exemple d'API DeleteObjectVersion suivant, remplacez les *`user input placeholders`* par vos propres informations.

```
DELETE /Key+?versionId=VersionId HTTP/1.1
Host: Bucket.s3.amazonaws.com
x-amz-mfa: MFA
x-amz-request-payer: RequestPayer
x-amz-bypass-governance-retention: BypassGovernanceRetention
x-amz-expected-bucket-owner: ExpectedBucketOwner
```

Si le demandeur restaure des objets à l'aide de l'API RestoreObject, le paiement par le demandeur est pris en charge tant que l'en-tête `x-amz-request-payer` ou le paramètre `RequestPayer` figure

dans la demande. Toutefois, le demandeur ne paiera que le coût de la demande. Le propriétaire du compartiment paiera les frais de récupération.

Les compartiments de type Paiement par le demandeur sont incompatibles avec ce qui suit.

- Les demandes anonymes
- Requêtes SOAP
- Utiliser un compartiment de paiement par le demandeur comme compartiment cible pour la journalisation de l'utilisateur final, ou vice versa. Toutefois, vous pouvez activer la journalisation de l'utilisateur final sur un compartiment de type Paiement par le demandeur lorsque le compartiment cible n'est pas un compartiment de type Paiement par le demandeur.

Fonctionnement du Paiement par le demandeur

La facturation des demandes de type Paiement par le demandeur est très simple : la demande et le transfert de données sont facturés au demandeur et le stockage des données est facturé au propriétaire du compartiment. Cependant, la demande est facturée au propriétaire du compartiment dans les cas suivants :

- La demande renvoie une erreur `AccessDenied` (HTTP`403 Forbidden`) et la demande est initiée au sein du AWS compte individuel ou de l' AWS organisation du propriétaire du bucket.
- si la demande est une demande SOAP.

Pour plus d'informations sur le paiement par le demandeur, consultez les rubriques suivantes.

Rubriques

- Configuration de Paiement par le demandeur sur un compartiment
- Récupération de la configuration requestPayment à l'aide de l'API REST
- Téléchargement d'objets à partir de compartiments de type Paiement par le demandeur

Configuration de Paiement par le demandeur sur un compartiment

Vous pouvez configurer un compartiment Amazon S3 comme compartiment de type Paiement par le demandeur afin que le demandeur paie à la place du propriétaire du compartiment le coût des demandes et des téléchargements des données.

Cette section fournit des exemples de configuration du Paiement par le demandeur sur un compartiment Amazon S3 à l'aide de la console et de l'API REST.

Utiliser la console S3.

Pour activer Requester Pays pour un compartiment S3 à usage général

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments à usage général, choisissez le nom du compartiment pour lequel vous souhaitez activer le paiement par le demandeur.
4. Choisissez Propriétés.
5. Sous Requester pays (Paiement par le demandeur), choisissez Edit (Modifier).
6. Choisissez Enable (Activer), puis Save changes (Enregistrer les modifications).

   Amazon S3 active le paiement par le demandeur pour le compartiment et affiche Bucket overview (Présentation du compartiment). Vous trouverez sous Paiement par le demandeur la mention Activé.

Utilisation de l'API REST

Seul le propriétaire du compartiment peut définir sa valeur de configuration `RequestPaymentConfiguration.payer` sur `BucketOwner` (valeur par défaut) ou sur `Requester`. La configuration de la ressource `requestPayment` est facultative. Par défaut, le compartiment n'est pas de type Paiement par le demandeur.

Pour désactiver la fonctionnalité Paiement par le demandeur et revenir à un compartiment standard, utilisez la valeur `BucketOwner`. En général, la valeur `BucketOwner` est utilisée lors du chargement des données dans le compartiment Amazon S3, et la valeur `Requester` est ensuite définie avant la publication des objets dans le compartiment.

Pour configurer requestPayment

- Utilisez une demande PUT pour définir la valeur `Payer` sur `Requester` dans un compartiment donné.

```
PUT ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
```

```
Content-Length: 173
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]

<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

Si la demande s'exécute correctement, Amazon S3 renvoie une réponse similaire à la suivante :

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Length: 0
Connection: close
Server: AmazonS3
x-amz-request-charged:requester
```

Vous pouvez définir le Paiement par le demandeur uniquement au niveau du regroupement. Vous ne pouvez pas définir le Paiement par le demandeur pour des objets spécifiques dans le compartiment.

Vous pouvez configurer un compartiment sur `BucketOwner` ou sur `Requester` à tout moment. Cependant, il peut y avoir quelques minutes avant que la nouvelle valeur de configuration ne prenne effet.

> **Note**
>
> Les propriétaires de compartiments qui distribuent des fichiers présignés URLs doivent y réfléchir attentivement avant de configurer un compartiment pour qu'il soit Requester Pays, en particulier si la durée de vie de l'URL est longue. En effet, le propriétaire du compartiment est facturé chaque fois qu'un demandeur utilise une URL pré-signée qui est associée aux informations d'identification du propriétaire du compartiment.

Récupération de la configuration requestPayment à l'aide de l'API REST

Vous pouvez demander la ressource `Payer` afin de connaître la valeur `requestPayment` définie pour un compartiment.

Pour obtenir la ressource requestPayment

- Utilisez une demande GET pour obtenir la ressource `requestPayment`, comme illustré dans la demande ci-dessous.

```
GET ?requestPayment HTTP/1.1
Host: [BucketName].s3.amazonaws.com
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

Si la demande s'exécute correctement, Amazon S3 renvoie une réponse similaire à la suivante :

```
HTTP/1.1 200 OK
x-amz-id-2: [id]
x-amz-request-id: [request_id]
Date: Wed, 01 Mar 2009 12:00:00 GMT
Content-Type: [type]
Content-Length: [length]
Connection: close
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<RequestPaymentConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
<Payer>Requester</Payer>
</RequestPaymentConfiguration>
```

Cette réponse montre que la valeur `payer` est définie sur `Requester`.

Téléchargement d'objets à partir de compartiments de type Paiement par le demandeur

Le téléchargement de données depuis les compartiments de type Paiement par le demandeur étant facturé aux demandeurs, les demandes doivent contenir un paramètre spécifique, `x-amz-request-payer`, qui confirme que les demandeurs savent que le téléchargement leur sera facturé. Pour accéder à des objets stockés dans un compartiment de type Paiement par le demandeur, les demandeurs doivent intégrer à leurs demandes l'un des paramètres suivants.

- Les demandes DELETE, GET, HEAD, POST et PUT doivent intégrer `x-amz-request-payer : requester` dans l'en-tête.

- Pour les documents signés URLs, `x-amz-request-payer=requester` incluez-les dans la demande

Lorsque la demande s'exécute correctement et que les frais sont facturés au demandeur, la réponse comprend l'en-tête `x-amz-request-charged:requester`. Si le paramètre `x-amz-request-payer` n'est pas inclus dans la demande, Amazon S3 renvoie une erreur 403 et la demande est facturée au propriétaire du compartiment.

> **Note**
>
> Il est inutile d'intégrer le paramètre `x-amz-request-payer` à vos demandes si vous être propriétaire du compartiment.
> En revanche, assurez-vous d'avoir intégré le paramètre `x-amz-request-payer` et la valeur qui lui est associée dans le calcul de la signature. Pour plus d'informations, consultez Utilisation d'un en-tête d'autorisation dans la Référence d'API Amazon S3.

Utilisation de l'API REST

Pour télécharger des objets depuis un compartiment de type Paiement par le demandeur

- Utilisez une demande `GET` pour télécharger un objet depuis un compartiment de type Paiement par le demandeur, comme illustré dans la demande ci-dessous.

```
GET / [destinationObject] HTTP/1.1
Host: [BucketName].s3.amazonaws.com
x-amz-request-payer : requester
Date: Wed, 01 Mar 2009 12:00:00 GMT
Authorization: AWS [Signature]
```

Lorsque la demande GET s'exécute correctement et que les frais sont facturés au demandeur, la réponse comprend `x-amz-request-charged:requester`.

Lorsque les demandes tentent d'obtenir un objet à partir d'un compartiment de type Paiement par le demandeur, il peut arriver qu'Amazon S3 renvoie une erreur `Access Denied`. Pour plus d'informations, consultez Réponses d'erreur dans la Référence d'API Amazon Simple Storage Service.

À l'aide du AWS CLI

Pour télécharger des objets depuis un bucket Requester Pays à l'aide du AWS CLI, vous le spécifiez dans `--request-payer requester` le cadre de votre `get-object` demande. Pour plus d'informations, consultez get-object dans la Référence des commandes AWS CLI .

Utilisation des objets dans Amazon S3

Pour stocker vos données dans Amazon S3, vous devez utiliser avec des ressources appelées compartiments et objets. Un compartiment est un conteneur d'objets. Un objet est un fichier et toutes les métadonnées qui le décrivent.

Pour stocker un objet dans Amazon S3, vous devez créer un compartiment, puis télécharger l'objet dans un compartiment. Lorsque l'objet se trouve dans le compartiment, vous pouvez l'ouvrir, le télécharger et le copier. Lorsque vous n'avez plus besoin d'un objet ou d'un compartiment, vous pouvez nettoyer ces ressources.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

> **Important**
>
> Dans la console Amazon S3, lorsque vous choisissez Ouvrir ou Télécharger comme pour un objet, ces opérations créent une signature présignée URLs. Pendant cinq minutes, votre objet sera accessible à toute personne ayant accès à ces objets présignés URLs. Pour plus d'informations sur les URL présignées URLs, consultez la section Utilisation d'URL présignées.

Avec Amazon S3, vous ne payez que les services que vous utilisez. Pour plus d'informations sur les fonctionnalités et les tarifs d'Amazon S3, consultez Amazon S3. Si vous êtes un nouveau client Amazon S3, vous pouvez commencer à utiliser Amazon S3 gratuitement. Pour plus d'informations, consultez la page sur l'offer gratuite AWS.

Rubriques

- Présentation des objets Amazon S3
- Attribution d'un nom aux objets Amazon S3
- Utilisation des métadonnées d'objet

- Chargement d'objets
- Ajout de conditions préalables aux opérations S3 avec des demandes conditionnelles
- Copie, déplacement et changement de nom des objets
- Téléchargement d'objets
- Vérification de l'intégrité des objets dans Amazon S3
- Suppression d'objets Amazon S3
- Organisation, liste et utilisation de vos objets
- Téléchargez et chargez des objets avec une signature préalable URLs
- Transformation d'objets avec S3 Object Lambda
- Exécution d'opérations groupées sur des objets avec les opérations par lot
- Interrogation des données sur place avec Amazon S3 Select

Présentation des objets Amazon S3

Amazon S3 est un magasin d'objets qui utilise des valeurs clés uniques pour stocker autant d'objets que vous le souhaitez. Vous stockez ces objets dans un ou plusieurs compartiments, et chaque objet peut atteindre 5 To. Un objet se compose des éléments suivants :

Clé

Nom que vous attribuez à un objet. Vous utilisez la clé de l'objet pour récupérer l'objet. Pour plus d'informations, consultez Utiliser les métadonnées d'un objet.

ID de version

Dans un compartiment, une clé et un ID de version identifient un objet de manière unique. L'ID de version est une chaîne de caractères générée par Amazon S3 lorsque vous ajoutez un objet à un compartiment. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Valeur

Contenu que vous stockez.

Une valeur d'objet peut être toute séquence d'octets. La taille des objets peut aller de zéro à 5 To. Pour plus d'informations, consultez Chargement d'objets.

Métadonnées

Ensemble de paires nom-valeur grâce auxquelles vous pouvez stocker des informations sur l'objet. Vous pouvez attribuer des métadonnées, appelées métadonnées définies par l'utilisateur, aux objets dans Amazon S3. Amazon S3 attribue également des métadonnées système à ces objets pour les gérer. Pour plus d'informations, consultez Utiliser les métadonnées d'un objet.

Sous-ressources

Amazon S3 utilise le mécanisme des sous-ressources pour stocker des informations supplémentaires propres à l'objet. Etant donné que les sous-ressources sont subordonnées aux objets, elles sont toujours associées à d'autres entités comme un objet ou un compartiment. Pour plus d'informations, consultez Sous-ressources d'objet.

Informations sur le contrôle d'accès

Vous pouvez contrôler l'accès aux objets que vous stockez dans Amazon S3. Amazon S3 prend en charge le contrôle d'accès basé sur les ressources, comme la liste de contrôle d'accès (ACL) et les stratégies de compartiment, ainsi que le contrôle d'accès basé sur l'utilisateur. Pour en savoir plus sur le contrôle d'accès, consultez la rubrique suivante :

- Contrôle d'accès dans Amazon S3
- Gestion des identités et des accès pour Amazon S3
- Configuration ACLs

Par défaut, vos ressources Amazon S3 (par exemple, les compartiments et les objets) sont privées. Vous devez accorder explicitement l'autorisation pour que d'autres utilisateurs accèdent aux ressources. Pour en savoir plus sur le partage d'objets, consultez Partage d'objets avec présigné URLs.

Balises

Vous pouvez utiliser des balises pour classer vos objets stockés par catégories à des fins de contrôle d'accès ou de répartition des coûts. Pour plus d'informations, consultez Catégorisation de vos objets à l'aide de balises.

Sous-ressources d'objet

Amazon S3 définit un ensemble de sous-ressources associées à des compartiments et à des objets. Les sous-ressources sont subordonnées aux objets. Cela signifie que les sous-ressources n'existent

pas par elles-mêmes. Elles sont toujours associées à une autre entité, comme un objet ou un compartiment.

Le tableau suivant répertorie les sous-ressources associées aux objets Amazon S3.

Sous-ressource	Description
liste acl	Contient une liste d'accords identifiant les bénéficiaires et les autorisations accordées. Lorsque vous créez un objet, la sous-ressource `acl` identifie le propriétaire de l'objet comme ayant le contrôle total sur l'objet. Vous pouvez récupérer la liste ACL d'un objet ou la remplacer par une liste mise à jour d'attributions. Toute mise à jour apportée à une liste ACL exige un remplacement de la liste ACL existante. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL).

Attribution d'un nom aux objets Amazon S3

La clé d'objet (ou nom de clé) identifie de façon unique l'objet dans un compartiment Amazon S3. Vous pouvez spécifier le nom d'une clé d'objet lors de la création de l'objet. Par exemple, dans la console Amazon S3, lorsque vous sélectionnez un compartiment, la liste des objets de ce compartiment s'affiche. Ces noms sont les clés d'objet.

Le nom de la clé de l'objet consiste en une séquence de caractères Unicode codés en UTF-8, d'une longueur maximale de 1 024 octets ou d'environ 1 024 caractères latins. Dans certaines langues, le codage d'un seul caractère peut nécessiter 2 octets. Lorsque vous nommez vos objets, tenez compte des points suivants :

- Les noms de clés d'objet ne sont pas sensibles à la casse.
- Les noms de clé d'objet incluent tous les préfixes (appelés dossiers dans la console). Par exemple, `Development/Projects.xls` est le nom complet de la clé d'objet de l'`Projects.xls`objet situé dans le `Development` préfixe (ou le dossier). Le préfixe, le délimiteur (`/`) et le nom de l'objet sont inclus dans la limite de 1 024 octets pour le nom de clé de l'objet. Pour plus d'informations sur les préfixes et les dossiers, consultezthe section called "Choix des noms de clés d'objet".
- Certains caractères peuvent nécessiter un traitement spécial lorsqu'ils sont utilisés dans les noms de clés d'objets. Pour de plus amples informations, veuillez consulter the section called "Directives de dénomination de la clé d'objet".

> **Note**
>
> Les noms de clé d'objet contenant la valeur `"soap"` ne sont pas pris en charge pour les virtual-hosted-style demandes. Pour les valeurs de nom de clé d'objet où `"soap"` il est utilisé, une URL de type chemin doit être utilisée à la place.

Choix des noms de clés d'objet

Le modèle de données Amazon S3 est une structure horizontale : vous créez un compartiment et ce compartiment stocke des objets. Il n'existe aucune hiérarchie de sous-compartiments ou de sous-dossiers. Toutefois, vous pouvez déduire une hiérarchie logique grâce aux préfixes et délimiteurs de nom de clé à l'image de la console Amazon S3. La console Amazon S3 prend en charge un concept de dossiers. Pour en savoir plus sur la modification des métadonnées à partir de la console Amazon S3, consultez Modification des métadonnées d'objet dans la console Amazon S3.

Imaginons que le compartiment (`admin-created`) comporte quatre objets avec les clés d'objet suivantes :

`Development/Projects.xls`

`Finance/statement1.pdf`

`Private/taxdocument.pdf`

`s3-dg.pdf`

La console utilise les préfixes de nom de clé (`Development/Finance/`, et`Private/`) et le délimiteur (`/`) pour présenter une structure de dossiers. La `s3-dg.pdf` clé ne contient pas de préfixe séparé par des barres obliques. Son objet apparaît donc directement à la racine du bucket. Si vous ouvrez le dossier `Development/`, vous voyez qu'il contient l'objet `Projects.xlsx`.

- Amazon S3 prend en charge les compartiments et les objets. Il n'y a aucune hiérarchie. Cependant, en utilisant des préfixes et des délimiteurs dans le nom d'une clé d'objet, la console Amazon S3 et le AWS SDKs peuvent déduire une hiérarchie et introduire le concept de dossiers.
- La console Amazon S3 implémente la création d'objets de dossier en créant un objet de type zéro octet avec la valeur préfixe et délimiteur du dossier comme clé. Ces objets de dossier n'apparaissent pas dans la console. Sinon, ils se comportent comme n'importe quel autre objet et peuvent être visualisés et manipulés via l'API REST, la AWS CLI et AWS SDKs.

Directives de dénomination de la clé d'objet

Vous pouvez utiliser n'importe quel caractère UTF-8 dans le nom de clé d'un objet. L'utilisation de certains caractères dans les noms de clé peut toutefois générer des problèmes avec certaines applications et certains protocoles. Les directives suivantes vous aident à optimiser la conformité avec le DNS, les caractères sécurisés pour le Web, les analyseurs XML, etc. APIs

Caractères adaptés

Les caractères configurés suivants sont généralement adaptés à une utilisation dans les noms de clés :

Caractères alphanumériques	• 0-9 • a-z • A-Z
Caractères spéciaux	• Point d'exclamation (!) • Trait d'union (-) • Trait de soulignement (_) • Point (.) • Astérisque (*) • Guillemet simple (') • Parenthèse ouvrante () (• Parenthèse fermante ())

Voici des exemples de noms de clés d'objet valides :

- `4my-organization`
- `my.great_photos-2014/jan/myvacation.jpg`
- `videos/2014/birthday/video1.wmv`

> **Note**
>
> Si vous utilisez la console Amazon S3 pour télécharger des objets dont les noms de clé se terminent par des `.` points (), les points sont supprimés de la fin des noms de clé des objets

téléchargés. Pour conserver les points à la fin des noms de clé dans les objets téléchargés, vous devez utiliser l'API REST AWS Command Line Interface (AWS CLI) ou Amazon S3. AWS SDKs

En outre, vous devez connaître les limitations suivantes en ce qui concerne les préfixes :

- Les objets avec un préfixe de `./` doivent être chargés ou téléchargés avec l'API AWS CLI, AWS SDKs, ou REST. Vous ne pouvez pas utiliser la console Amazon S3 pour télécharger ces objets.
- Les clés d'objet contenant des éléments de chemin relatifs (par exemple, `../`) sont valides si, lors de l'analyse left-to-right, le nombre cumulé de segments de chemin relatifs ne dépasse jamais le nombre d'éléments de chemin non relatifs rencontrés. Cette règle s'applique à toutes les demandes effectuées à l'aide de la console Amazon S3, de l'API REST Amazon S3 et AWS SDKs. AWS CLI

  Par exemple :

  - `videos/2014/../../video1.wmv`est valide.
  - `videos/../../video1.wmv`n'est pas valide.
  - `videos/../../2014/video1.wmv`n'est pas valide.

Caractères pouvant exiger une manipulation spéciale

Les caractères suivants d'un nom de clé peuvent nécessiter une gestion de code supplémentaire et doivent très probablement être codés en URL ou référencés au format HEX. Certains de ces caractères sont des caractères non imprimables que votre navigateur risque de ne pas gérer et qui nécessitent également un traitement spécial :

- Esperluette () &
- Signe du dollar ($)
- Les caractères ASCII 00–1F hex (0–31 décimale) et 7F (127 décimale)
- Symbole d'art (@)
- Signe égal (=)
- Point-virgule () `;`
- Barre oblique (`/`)
- Colon (`:`)

- Signe Plus (+)
- Espace — Des séquences d'espaces importantes peuvent être perdues dans certains cas (en particulier plusieurs espaces)
- Virgule (,)
- Point d'interrogation (?)

Caractères à éviter

Nous vous recommandons de ne pas utiliser les caractères suivants dans le nom d'une clé en raison de la gestion importante des caractères spéciaux, qui n'est pas uniforme dans toutes les applications :

- Barre oblique inverse (\)
- Orthèse gauche ({)
- Caractères ASCII non imprimables (128–255 caractères décimaux)
- Caret ou circonflexe (^)
- Orthèse droite (})
- Pourcentage de caractères (%)
- Accent grave ou backtick (`)
- Support droit (])
- Guillemet (")
- Plus grand que le signe (>)
- Support gauche ([)
- Tilde (~)
- Moins que le signe (<)
- Signe de la livre (#)
- Barre ou tuyau vertical (|)

Contraintes relatives aux clés d'objets liées au XML

Comme spécifié par la norme XML relative à la end-of-line manipulation, tout le texte XML est normalisé de telle sorte que les retours d'un seul chariot (code ASCII 13) et les retours de chariot

immédiatement suivis d'un fil (code ASCII 10), également appelés caractères de nouvelle ligne, sont remplacés par un caractère d'alimentation d'une seule ligne. Pour garantir l'analyse correcte des clés d'objet dans les demandes XML, les retours de transport et les autres caractères spéciaux doivent être remplacés par leur code d'entité XML équivalent lorsqu'ils sont insérés dans des balises XML.

Voici une liste de ces caractères spéciaux et de leurs codes d'entité XML équivalents :

- L'apostrophe (') doit être remplacée par `'`
- Le guillemet (") doit être remplacé par `"`
- L'esperluette (&) doit être remplacée par `&`
- Le signe inférieur à (<) doit être remplacé par `<`
- Le signe supérieur à (>>) doit être remplacé par `>`
- Le retour du chariot (`\r`) doit être remplacé par `
` ou `
`
- Newline (`\n`) doit être remplacé par ou `
` `
`

Example

L'exemple suivant montre l'utilisation d'un code d'entité XML à la place d'un retour chariot. Cette `DeleteObjects` demande supprime un objet avec le `key` paramètre `/some/prefix/objectwith\rcarriagereturn` (où il `\r` s'agit du retour du chariot).

```
<Delete xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Object>
    <Key>/some/prefix/objectwith&#13;carriagereturn</Key>
  </Object>
</Delete>
```

Utilisation des métadonnées d'objet

Il existe deux types de métadonnées d'objet dans Amazon S3 : les métadonnées définies par le système et les métadonnées définies par l'utilisateur. Les métadonnées définies par le système incluent des informations telles que la date de création de l'objet, sa taille et sa classe de stockage. Les métadonnées définies par l'utilisateur sont des informations que vous pouvez choisir de définir au moment du chargement d'un objet. Il s'agit d'un ensemble de paires nom-valeur. Pour plus d'informations, consultez the section called "Métadonnées d'objet définies par le système" et the section called "Métadonnées d'objet définies par l'utilisateur".

Lorsque vous créez un objet, vous spécifiez la clé d'objet, aussi appelée nom de clé, qui identifie de façon unique l'objet dans un compartiment Amazon S3. Pour de plus amples informations, veuillez consulter Attribution d'un nom aux objets Amazon S3. Vous pouvez définir les métadonnées définies par l'utilisateur dans Amazon S3 au moment du chargement de l'objet.

Une fois l'objet chargé, vous ne pourrez plus modifier ces métadonnées définies par l'utilisateur. Le seul moyen de modifier ces métadonnées consisterait à copier l'objet et à en configurer les métadonnées. Pour plus d'informations sur la modification des métadonnées à l'aide de la console Amazon S3, consultez Modification des métadonnées d'objet dans la console Amazon S3.

Interrogation de vos métadonnées et accélération de la découverte des données avec les métadonnées S3

Pour trouver, stocker et interroger facilement les métadonnées de vos objets S3, vous pouvez utiliser les métadonnées S3. Avec les métadonnées S3, vous pouvez rapidement préparer des données pour les utiliser dans l'analytique métier, l'extraction de contenu, l'entraînement des modèles d'intelligence artificielle et de machine learning (IA/ML), etc.

Les métadonnées S3 accélèrent la découverte des données en capturant automatiquement les métadonnées des objets de vos compartiments à usage général et en les stockant dans des tables Apache Iceberg entièrement gérées en lecture seule que vous pouvez interroger. Ces tables en lecture seule sont appelées tables de métadonnées. Lorsque des objets sont ajoutés, mis à jour ou supprimés dans vos compartiments à usage général, les métadonnées S3 actualisent automatiquement les tables de métadonnées correspondantes pour refléter les dernières modifications.

Par défaut, les métadonnées S3 fournissent les métadonnées d'objet définies par le système, telles que l'heure de création et la classe de stockage d'un objet, et les métadonnées personnalisées, telles que les balises et les métadonnées définies par l'utilisateur qui ont été incluses lors du chargement de l'objet. S3 Metadata fournit également des métadonnées d'événements, par exemple lorsqu'un objet est mis à jour ou supprimé, et Compte AWS l'auteur de la demande.

Les tables de métadonnées sont stockées dans des compartiments de tables S3, qui fournissent un stockage optimisé pour les données tabulaires. Pour interroger vos métadonnées, vous pouvez intégrer votre compartiment de tables à des services AWS d'analyse tels qu'Amazon Athena, Amazon Redshift et Amazon. QuickSight

Pour en savoir plus sur les métadonnées S3, consultez the section called "Accélération de la découverte des données".

Métadonnées d'objet définies par le système

Pour chaque objet stocké dans un compartiment, Amazon S3 gère un ensemble de métadonnées système. Amazon S3 traite ces métadonnées système selon les besoins. Par exemple, Amazon S3 gère les métadonnées liées à la date de création et à la taille de l'objet et utilise ces informations dans le cadre de la gestion des objets.

Il existe deux classes de métadonnées système :

- Contrôlées par le système : les métadonnées comme la date de création de l'objet sont contrôlées par le système. Par conséquent, seul Amazon S3 peut modifier la valeur de date.
- Contrôlées par l'utilisateur : les autres métadonnées système, comme la classe de stockage configurée pour l'objet et l'activation du chiffrement côté serveur dans l'objet, sont des exemples de métadonnées système dont vous contrôlez la valeur. Si le compartiment est configuré en tant que site web, il se peut que vous souhaitiez rediriger une demande de page vers une autre page ou une URL externe. Dans ce cas, une page Web est un objet dans le compartiment. Amazon S3 stocke la valeur de redirection de la page en tant que métadonnées système que vous pouvez contrôler.

  Lorsque vous créez des objets, vous pouvez configurer les valeurs de ces éléments de métadonnées système ou mettre à jour les valeurs le cas échéant. Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

  Amazon S3 utilise des AWS KMS clés pour chiffrer vos objets Amazon S3. AWS KMS chiffre uniquement les données de l'objet. La somme de contrôle et l'algorithme spécifié sont stockés dans le cadre des métadonnées de l'objet. Si un chiffrement côté serveur est demandé pour l'objet, le total de contrôle est stocké sous forme chiffrée. Pour plus d'informations sur le chiffrement côté serveur, consultez Protection des données à l'aide du chiffrement.

> **Note**
>
> L'en-tête de la demande PUT est limité à une taille de 8 Ko. Dans l'en-tête de la demande PUT, les métadonnées définies par le système sont limitées à une taille de 2 Ko. La taille des métadonnées définies par le système est mesurée grâce à la somme des octets dans l'encodage US-ASCII de chaque clé et valeur.

Le tableau suivant fournit une liste des métadonnées définies par le système et indique si elles peuvent être mises à jour.

Nom	Description	L'utilisateur peut-il modifier la valeur ?
`Date`	Les date et heure actuelles.	Non
`Cache-Control`	Champ d'en-tête général utilisé pour spécifier les stratégies de mise en cache.	Oui
`Content-Disposition`	Informations de présentation des objets.	Oui
`Content-Length`	La taille des objets en octets.	Non
`Content-Type`	Le type d'objet.	Oui
`Last-Modified`	La date de création ou de dernière modification, la plus récente des deux. Pour les chargements partitionnés, la date de création de l'objet correspond à la date de lancement du chargement partitionné.	Non
`ETag`	Une étiquette d'entité (ETag) qui représente une version spécifique d'un objet. Pour les objets qui ne sont pas chargés en plusieurs parties et qui sont soit non chiffrés, soit chiffrés par chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), il s' ETag agit d'un condensé des données. MD5	Non
`x-amz-server-side-encryption`	En-tête qui indique si le chiffrement côté serveur est activé pour l'objet et si ce chiffrement utilise les clés AWS Key Management Service (AWS KMS) (SSE-KMS) ou les clés de chiffrement gérées par Amazon S3 (SSE-S3). Pour de plus amples informations, veuillez consulter Protection des données avec le chiffrement côté serveur.	Oui

Nom	Description	L'utilisateur peut-il modifier la valeur ?
`x-amz-checksum-crc64nvme` , `x-amz-checksum-crc32` , `x-amz-checksum-crc32c` , `x-amz-checksum-sha1` , `x-amz-checksum-sha256`	Des en-têtes qui contiennent le total de contrôle ou le récapitulatif de l'objet. Au maximum, un de ces en-têtes sera défini à la fois, en fonction de l'algorithme de total de contrôle que vous demandez à Amazon S3 d'utiliser. Pour plus d'informations sur la façon de sélectionner l'algorithme de total de contrôle, consultez Vérification de l'intégrité des objets dans Amazon S3.	Non
`x-amz-checksum-type`	Type de somme de contrôle, qui détermine la manière dont les sommes de contrôle au niveau de chaque partie sont combinées pour créer une somme de contrôle au niveau de l'objet pour les objets en plusieurs parties.	Oui
`x-amz-version-id`	La version d'un objet. Lorsque vous activez la gestion des versions sur un compartiment, Amazon S3 attribue un ID de version aux objets ajoutés au compartiment. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.	Non
`x-amz-delete-marker`	Un marqueur booléen qui indique si l'objet est un marqueur de suppression. Ce marqueur n'est utilisé que dans les compartiments pour lesquels la gestion des versions est activée.	Non
`x-amz-storage-class`	La classe de stockage utilisée pour stocker l'objet. Pour plus d'informations, consultez Bien comprendre et gérer les classes de stockage Amazon S3.	Oui

Nom	Description	L'utilisateur peut-il modifier la valeur ?
`x-amz-website-redirect-location`	Un en-tête qui redirige les demandes pour l'objet associé vers un autre objet dans le même compartiment ou une URL externe. Pour plus d'informations, consultez (Facultatif) Configuration de la redirection de pages web.	Oui
`x-amz-server-side-encryption-aws-kms-key-id`	En-tête qui indique l'ID de la clé KMS de chiffrement AWS KMS symétrique utilisée pour chiffrer l'objet. Cet en-tête est utilisé uniquement lorsque l'en-tête `x-amz-server-side-encryption` est présent et a la valeur de `aws:kms`.	Oui
`x-amz-server-side-encryption-customer-algorithm`	Un en-tête qui indique si le chiffrement côté serveur à l'aide des clés de chiffrement fournies par le client (SSE-C) est activé. Pour plus d'informations, consultez Utilisation du chiffrement côté serveur avec les clés fournies par le client (SSE-C).	Oui
`x-amz-tagging`	Ensemble de balises de l'objet. L'ensemble de balises doit être codé en tant que paramètres de requête URL.	Oui

Métadonnées d'objet définies par l'utilisateur

Lorsque vous chargez un objet, vous pouvez également lui attribuer des métadonnées. Vous fournissez ces informations facultatives en tant que paire nom-valeur (clé-valeur) lorsque vous envoyez une demande PUT ou POST pour créer l'objet. Lors du chargement des objets grâce à l'API REST, les noms facultatifs des métadonnées définies par l'utilisateur doivent commencer par « `x-amz-meta-` » pour se différencier des autres en-têtes HTTP. Lorsque vous récupérez l'objet grâce à l'API REST, ce préfixe est renvoyé. Lors du chargement des objets grâce à l'API SOAP, le préfixe n'est pas requis. Lorsque vous récupérez l'objet grâce à l'API SOAP, le préfixe est supprimé, quelle que soit l'API utilisée pour charger l'objet.

> **Note**
>
> Les SOAP APIs pour Amazon S3 ne sont pas disponibles pour les nouveaux clients et approchent de leur fin de vie (EOL) le 31 août 2025. Nous vous recommandons d'utiliser l'API REST ou le AWS SDKs.

Lorsque des métadonnées sont récupérées via l'API REST, Amazon S3 associe les en-têtes avec le même nom (sans tenir compte de la casse) dans une liste séparée par des virgules. Si certaines métadonnées contiennent des caractères non imprimables, elles ne sont pas renvoyées. À la place, l'en-tête `x-amz-missing-meta` est renvoyé avec le nombre d'entrées de métadonnées non imprimables. L'action `HeadObject` récupère les métadonnées d'un objet sans retourner l'objet lui-même. Cette opération est pratique si vous êtes uniquement intéressé par les métadonnées d'un objet. Pour utiliser `HEAD`, vous devez disposer d'un accès `READ` sur l'objet. Pour plus d'informations, consultez HeadObjectle manuel Amazon Simple Storage Service API Reference.

Les métadonnées définies par l'utilisateur sont un ensemble de paires de clés-valeurs. Amazon S3 stocke les clés de métadonnées définies par l'utilisateur en minuscules.

Amazon S3 accepte les caractères Unicode arbitraires dans vos valeurs de métadonnées.

Pour éviter des problèmes liés à la présentation de ces valeurs de métadonnées, vous devez vous conformer à l'utilisation de caractères US-ASCII avec REST et UTF-8 lors de l'utilisation de SOAP ou de chargements basés sur un navigateur via `POST`.

Lorsque vous utilisez non-US-ASCII des caractères dans vos valeurs de métadonnées, la chaîne Unicode fournie est examinée pour détecter les non-US-ASCII caractères. Les valeurs de ces en-têtes sont décodées en caractères selon la RFC 2047 avant d'être stockées, puis encodées selon la RFC 2047 pour qu'elles soient transmises de manière sécurisée par e-mail avant d'être renvoyées. Si la chaîne contient uniquement des caractères US-ASCII, elle est présentée telle qu'elle est.

Voici un exemple.

```
PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: ÄMÄZÕÑ S3

HEAD /Key HTTP/1.1
```

```
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-nonascii: =?UTF-8?B?w4PChE3Dg8KEWsODwpXDg8KRIFMz?=

PUT /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3

HEAD /Key HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
x-amz-meta-ascii: AMAZONS3
```

> **Note**
>
> L'en-tête de la demande PUT est limité à une taille de 8 Ko. Dans l'en-tête de la demande PUT, les métadonnées définies par l'utilisateur sont limitées à une taille de 2 Ko. La taille des métadonnées définies par l'utilisateur est mesurée grâce à la somme des octets dans l'encodage UTF-8 de chaque clé et valeur.

Pour plus d'informations sur la modification des métadonnées de votre objet après son téléchargement, en créant une copie de l'objet, en le modifiant et en remplaçant l'ancien objet, ou en créant une version, consultez Modification des métadonnées d'objet dans la console Amazon S3.

Modification des métadonnées d'objet dans la console Amazon S3

Vous pouvez utiliser la console Amazon S3 pour modifier les métadonnées des objets S3 existants en utilisant l'action Copier. Pour modifier les métadonnées, copiez les objets vers la même destination et spécifiez les nouvelles métadonnées que vous souhaitez appliquer, qui remplaceront les anciennes métadonnées de l'objet. Certaines métadonnées sont définies par Amazon S3 lorsque vous chargez l'objet. Par exemple, `Content-Length` et `Last-Modified` sont des champs de métadonnées d'objet définies par le système qui ne peuvent pas être modifiés par un utilisateur.

Vous pouvez également définir des métadonnées définies par l'utilisateur lorsque vous chargez l'objet et les remplacer á mesure que vos besoins évoluent. Par exemple, vous pouvez avoir un ensemble d'objets que vous stockez initialement dans la classe de stockage `STANDARD`. Au fil du temps, vous n'aurez peut-être plus besoin que ces données soient hautement disponibles. Vous pourrez donc remplacer la classe de stockage par `GLACIER` en faisant passer la valeur de la clé `x-amz-storage-class` `STANDARD` à `GLACIER`.

Note

Tenez compte des points suivants lorsque vous modifiez des métadonnées d'objet dans Amazon S3 :

- Vous devez spécifier les métadonnées existantes que vous souhaitez conserver, les métadonnées que vous souhaitez ajouter et les métadonnées que vous souhaitez modifier.
- Si la taille de l'objet est inférieure à 5 Go, vous pouvez utiliser l'action Copier dans la console S3 pour remplacer les métadonnées de l'objet. Si la taille de votre objet est supérieure à 5 Go, vous pouvez remplacer les métadonnées de l'objet lorsque vous copiez un objet avec un téléchargement partitionné en utilisant le AWS CLIou AWS SDKs. Pour de plus amples informations, veuillez consulter Copie d'un objet à l'aide du chargement partitionné.
- Pour obtenir une liste des autorisations supplémentaires requises pour remplacer les métadonnées, consultez the section called "Autorisations requises pour les opérations d'API S3". Pour obtenir un exemple de politiques qui accorde ces autorisations, consultez the section called "Exemples de politiques basées sur l'identité".
- Cette action crée une copie de l'objet avec les paramètres mis à jour et la date de la dernière modification. Si la gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Si le contrôle de version S3 n'est pas activé, une nouvelle copie de l'objet remplace l'objet d'origine. Le rôle IAM Compte AWS associé qui modifie la propriété devient également propriétaire du nouvel objet ou (version de l'objet).
- La modification des métadonnées remplace les valeurs des noms de clés existants.
- Les objets chiffrés à l'aide des clés de chiffrement fournies par le client (SSE-C) ne peuvent pas être copiés à l'aide de la console. Vous devez utiliser AWS CLI le AWS SDK ou l'API REST Amazon S3.
- Lorsque vous copiez un objet à l'aide de la console Amazon S3, vous pouvez recevoir le message d'erreur « Les métadonnées copiées ne peuvent pas être vérifiées ». La console utilise des en-têtes pour récupérer et définir les métadonnées de votre objet. Si la configuration de votre réseau ou de votre navigateur modifie vos requêtes réseau, ce comportement peut entraîner l'écriture involontaire de métadonnées (telles que `Cache-Control` des en-têtes modifiés) dans l'objet copié. Amazon S3 ne peut pas vérifier ces métadonnées involontaires.

Pour résoudre ce problème, vérifiez la configuration de votre réseau et de votre navigateur pour vous assurer qu'elle ne modifie pas les en-têtes, tels que`Cache-Control`. Pour plus d'informations, consultez le modèle de responsabilité partagée.

> **Warning**
>
> Lorsque vous remplacez les métadonnées d'un dossier, attendez la fin de l'action Copier avant d'ajouter de nouveaux objets à ce dossier. Sinon, de nouveaux objets peuvent également être modifiés.

Les rubriques suivantes décrivent comment remplacer les métadonnées d'un objet à l'aide de l'action Copier dans la console Amazon S3.

Remplacement de métadonnées définies par le système

Vous pouvez remplacer certaines métadonnées définies par le système pour un objet S3. Pour obtenir la liste des métadonnées définies par le système et des valeurs que vous pouvez modifier, consultez Métadonnées d'objet définies par le système.

Pour remplacer les métadonnées définies par le système pour un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant les objets que vous souhaitez modifier.
4. Cochez la case correspondant aux objets à modifier.
5. Dans le menu Actions, choisissez Copier à partir de la liste d'options qui s'affiche.
6. Pour spécifier le chemin de destination, choisissez Parcourir S3, accédez à la destination des objets sources, puis cochez la case Destination. Choisissez Choose destination (Choisir une destination) en bas à droite.

   Vous pouvez également saisir le chemin de destination.

7. Si la gestion des versions n'est pas activée au niveau des compartiments, un avertissement vous recommande de l'activer afin de vous protéger contre le remplacement ou la suppression involontaires d'objets. Si vous souhaitez conserver toutes les versions des objets dans ce compartiment, sélectionnez Enable Bucket Versioning (Activer la gestion des versions pour le compartiment). Vous pouvez également consulter les propriétés de chiffrement et de verrouillage des objets par défaut dans Détails de la destination.
8. Sous Paramètres de copie supplémentaires, choisissez Spécification des paramètres pour définir les paramètres des métadonnées.
9. Accédez à la section Métadonnées, puis choisissez Remplacer toutes les métadonnées.
10. Sélectionnez Ajouter des métadonnées.
11. Pour Type de métadonnées, sélectionnez Définies par le système.
12. Spécifiez une valeur Clé unique et renseignez le champ Valeur des métadonnées.
13. Pour modifier des métadonnées supplémentaires, choisissez Ajouter des métadonnées. Vous pouvez également choisir Supprimer pour supprimer un ensemble de type-key-values.
14. Choisissez Copier. Amazon S3 enregistre les modifications apportées aux métadonnées.

Remplacement de métadonnées définies par l'utilisateur

Pour remplacer les métadonnées définies par l'utilisateur pour un objet spécifique, combinez le préfixe de métadonnées, `x-amz-meta-`, et un nom que vous choisissez pour créer une clé personnalisée. Par exemple, si vous ajoutez le nom personnalisé `alt-name`, la clé de métadonnées est `x-amz-meta-alt-name`.

Les métadonnées définies par l'utilisateur peuvent atteindre 2 Ko. Pour calculer la taille totale des métadonnées définies par l'utilisateur, additionnez le nombre d'octets dans l'encodage UTF-8 pour chaque clé et valeur. Les clés et leurs valeurs doivent respecter les normes US-ASCII. Pour de plus amples informations, veuillez consulter Métadonnées d'objet définies par l'utilisateur.

Pour remplacer des métadonnées définies par l'utilisateur pour un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments, puis l'onglet Compartiments à usage général ou Compartiments de répertoires. Accédez au compartiment ou au dossier Amazon S3 contenant les objets que vous souhaitez modifier.
3. Cochez la case correspondant aux objets à modifier.

4. Dans le menu Actions, choisissez Copier à partir de la liste d'options qui s'affiche.
5. Pour spécifier le chemin de destination, choisissez Parcourir S3, accédez à la destination des objets sources, puis cochez la case Destination. Choisissez Choose destination (Choisir une destination).

   Vous pouvez également saisir le chemin de destination.
6. Si la gestion des versions n'est pas activée au niveau des compartiments, un avertissement vous recommande de l'activer afin de vous protéger contre le remplacement ou la suppression involontaires d'objets. Si vous souhaitez conserver toutes les versions des objets dans ce compartiment, sélectionnez Enable Bucket Versioning (Activer la gestion des versions pour le compartiment). Vous pouvez également consulter les propriétés de chiffrement et de verrouillage des objets par défaut dans Détails de la destination.
7. Sous Paramètres de copie supplémentaires, choisissez Spécification des paramètres pour définir les paramètres des métadonnées.
8. Accédez à la section Métadonnées, puis choisissez Remplacer toutes les métadonnées.
9. Sélectionnez Ajouter des métadonnées.
10. Pour le Type de métadonnées, choisissez Définies par l'utilisateur.
11. Renseignez le champ Cléavec une clé personnalisée unique au format `x-amz-meta-`. Renseignez également le champ Valeur pour les métadonnées.
12. Pour ajouter des métadonnées supplémentaires, choisissez Ajouter des métadonnées. Vous pouvez également choisir Supprimer pour supprimer un ensemble de type-key-values.
13. Choisissez Copier. Amazon S3 enregistre les modifications apportées aux métadonnées.

Accélération de la découverte des données avec les métadonnées S3

Amazon S3 Metadata accélère la découverte des données en capturant automatiquement les métadonnées des objets de vos compartiments à usage général et en les stockant dans des Apache Iceberg tables entièrement gérées en lecture seule que vous pouvez interroger. Ces tables en lecture seule sont appelées tables de métadonnées. Lorsque des objets sont ajoutés, mis à jour ou supprimés de vos compartiments à usage général, S3 Metadata actualise automatiquement les tables de métadonnées correspondantes pour refléter les dernières modifications.

Par défaut, les métadonnées S3 fournissent trois types de métadonnées :

- Métadonnées définies par le système, telles que l'heure de création et la classe de stockage d'un objet

- Métadonnées personnalisées, telles que les balises et les métadonnées définies par l'utilisateur qui ont été incluses lors du chargement de l'objet
- Les métadonnées des événements, par exemple lorsqu'un objet est mis à jour ou supprimé, et Compte AWS l'auteur de la demande

Avec les métadonnées S3, vous pouvez facilement rechercher, stocker et interroger les métadonnées de vos objets S3, afin de préparer rapidement les données à utiliser dans l'analytique métier, l'extraction de contenu, l'entraînement des modèles d'intelligence artificielle et de machine learning (IA/ML), etc.

Pour chaque compartiment à usage général, vous pouvez créer une configuration de table de métadonnées contenant deux tables de métadonnées complémentaires :

- Table de journal : par défaut, la configuration de votre table de métadonnées contient une table de journal qui capture les événements qui se produisent pour les objets de votre compartiment. Le tableau du journal enregistre les modifications apportées à vos données en temps quasi réel, ce qui vous aide à identifier les nouvelles données téléchargées dans votre bucket, à suivre les objets récemment supprimés, à surveiller les transitions du cycle de vie, etc. La table du journal enregistre les nouveaux objets et les mises à jour de vos objets et de leurs métadonnées (mises à jour nécessitant une opération `PUT` ou une `DELETE` opération).

  La table de journal capture les métadonnées uniquement pour les événements de modification (tels que les téléchargements, les mises à jour et les suppressions) qui se produisent après la création de la configuration de votre table de métadonnées. Comme cette table peut être interrogée, vous pouvez auditer les modifications apportées à votre bucket par le biais de simples requêtes SQL.

  La table de journal est obligatoire pour chaque configuration de table de métadonnées. (Dans la version initiale de S3 Metadata, la table de journal était appelée « table de métadonnées ».)

  Pour plus d'informations sur les données stockées dans les tables de journal, voirthe section called "Schéma des tables de journaux".

  Pour minimiser vos coûts de stockage, vous pouvez choisir d'activer l'expiration des enregistrements de la table de journal. Pour de plus amples informations, veuillez consulter the section called "Enregistrements de table de journal expirant".
- Table d'inventaire dynamique : vous pouvez éventuellement ajouter une table d'inventaire dynamique à la configuration de votre table de métadonnées. Le tableau d'inventaire en temps

réel fournit un inventaire simple et interrogeable de tous les objets et de leurs versions dans votre compartiment afin que vous puissiez déterminer l'état le plus récent de vos données.

Vous pouvez utiliser le tableau d'inventaire en temps réel pour simplifier et accélérer les flux de travail commerciaux et les tâches liées au Big Data en identifiant les objets que vous souhaitez traiter pour différentes charges de travail. Par exemple, vous pouvez interroger la table d'inventaire dynamique pour trouver tous les objets stockés dans une classe de stockage donnée, tous les objets dotés de certaines balises, tous les objets qui ne sont pas chiffrés par chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS), etc.

Lorsque vous activez la table d'inventaire dynamique pour la configuration de votre table de métadonnées, la table est soumise à un processus appelé backfilling, au cours duquel Amazon S3 analyse votre compartiment à usage général pour récupérer les métadonnées initiales de tous les objets présents dans le compartiment. Selon le nombre d'objets contenus dans votre compartiment, ce processus peut prendre de quelques minutes (minimum 15 minutes) à plusieurs heures. Lorsque le processus de remblayage est terminé, le statut de votre tableau d'inventaire en temps réel passe de Remblayage à Actif. Une fois le remblayage terminé, les mises à jour apportées à vos objets sont généralement reflétées dans le tableau d'inventaire en temps réel en moins d'une heure.

Le remplissage de votre tableau d'inventaire vous est facturé. Si votre bucket à usage général contient plus d'un milliard d'objets, des frais mensuels vous sont également facturés pour votre tableau d'inventaire en ligne. Pour plus d'informations, consultez Tarification Amazon S3.

Pour plus d'informations sur les données stockées dans les tables d'inventaire dynamiques, consultezthe section called “Schéma des tables d'inventaire en temps réel”.

Vos tables de métadonnées sont stockées dans un compartiment de tables S3 AWS géré, qui fournit un stockage optimisé pour les données tabulaires. Pour interroger vos métadonnées, vous pouvez intégrer votre bucket de table à Amazon SageMaker Lakehouse. Cette intégration, qui utilise le AWS Glue Data Catalog et AWS Lake Formation, permet aux services AWS d'analyse de découvrir et d'accéder automatiquement aux données de votre table.

Une fois votre compartiment de tables intégré au AWS Glue Data Catalog, vous pouvez directement interroger vos tables de métadonnées à l'aide de services AWS d'analyse tels qu'Amazon Athena, Amazon EMR et Amazon Redshift. Vous pouvez également créer des tableaux de bord interactifs avec les données de vos requêtes à l'aide d'Amazon QuickSight. Pour plus d'informations sur

l'intégration de votre compartiment de table S3 AWS géré à Amazon SageMaker Lakehouse, consultez. the section called “Utilisation de tables S3 avec des services AWS d'analyse”

Vous pouvez également interroger vos tables de métadonnées avec Apache SparkApache Trino, et toute autre application prenant en charge le Apache Iceberg format en utilisant le point de terminaison AWS Glue Iceberg REST, le point de terminaison Iceberg REST Amazon S3 Tables ou le catalogue de tables Amazon S3 pour le catalogue Apache Iceberg client. Pour plus d'informations sur l'accès à vos tables de métadonnées, consultezthe section called “Accès aux tables”.

Pour en savoir plus sur la tarification des métadonnées S3, consultez Tarification Amazon S3.

Fonctionnement des tables de métadonnées

Les tables de métadonnées sont gérées par Amazon S3 et ne peuvent être modifiées par aucun principal IAM en dehors d'Amazon S3 lui-même. Vous pouvez toutefois supprimer vos tables de métadonnées. Par conséquent, les tables de métadonnées sont en lecture seule, ce qui permet de garantir qu'elles reflètent correctement le contenu de votre bucket à usage général.

Pour générer et stocker des métadonnées d'objets dans des tables de métadonnées AWS gérées, vous devez créer une configuration de table de métadonnées pour votre bucket à usage général. Amazon S3 est conçu pour mettre à jour en permanence les tables de métadonnées afin de refléter les dernières modifications apportées à vos données tant que la configuration est active sur le compartiment à usage général.

Avant de créer une configuration de table de métadonnées, assurez-vous que vous disposez des autorisations AWS Identity and Access Management (IAM) nécessaires pour créer et gérer des tables de métadonnées. Pour de plus amples informations, veuillez consulter the section called “Autorisations pour les tables de métadonnées”.

Stockage, organisation et chiffrement des tables de métadonnées

Lorsque vous créez la configuration de vos tables de métadonnées, celles-ci sont stockées dans un bucket de tables AWS géré. Toutes les configurations de tables de métadonnées de votre compte et de la même région sont stockées dans un seul compartiment de table AWS géré. Ces compartiments de tables AWS gérés sont nommés `aws-s3` et ont le format Amazon Resource Name (ARN) suivant :

```
arn:aws:s3tables:region:account_id:bucket/aws-s3
```

Par exemple, si votre identifiant de compte est 123456789012 et que votre compartiment à usage général se trouve dans l'est des États-Unis (Virginie du Nord) (`us-east-1`), votre compartiment de

table AWS géré est également créé dans l'est des États-Unis (Virginie du Nord) (`us-east-1`) et possède l'ARN suivant :

`arn:aws:s3tables:`*`us-east-1`*`:123456789012:bucket/aws-s3`

Par défaut, les compartiments de tables AWS gérés sont chiffrés par chiffrement côté serveur à l'aide de clés gérées Amazon S3 (SSE-S3). Après avoir créé votre première configuration de métadonnées, vous pouvez définir le paramètre de chiffrement par défaut pour le compartiment de table AWS géré afin d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Pour plus d'informations, consultez les sections Chiffrement pour les compartiments de tables AWS gérés etthe section called "Spécification de SSE-KMS".

Dans votre compartiment de tables AWS géré, les tables de métadonnées de votre configuration sont généralement stockées dans un espace de noms au format de dénomination suivant :

b_*general-purpose-bucket-name*

> **Note**
>
> - Si le nom de votre bucket à usage général contient des points, ceux-ci sont convertis en traits de soulignement (_) dans le nom de l'espace de noms.
> - Si votre bucket à usage général a été créé avant le 1er mars 2018, son nom peut contenir des lettres majuscules et des traits de soulignement, et il peut également comporter jusqu'à 255 caractères. Si le nom de votre bucket possède ces caractéristiques, l'espace de noms de votre table de métadonnées aura un format différent. Le nom du compartiment à usage général sera préfixéb_, tronqué à 63 caractères, converti en minuscules et suffixé d'un hachage.

Les tables de métadonnées possèdent le format d'Amazon Resource Name (ARN) suivant :

`arn:aws:s3tables:`*`region-code`*`:`*`account-id`*`:bucket/aws-s3/table/`*`metadata_table_name`*

Les tables de journal portent le nom `journal` et les tables d'inventaire dynamiques portent le nom`inventory`.

Lorsque vous créez la configuration de votre table de métadonnées, vous pouvez choisir de chiffrer vos tables de métadonnées AWS gérées avec un chiffrement côté serveur à l'aide de clés AWS

Key Management Service (AWS KMS) (SSE-KMS). Si vous choisissez d'utiliser SSE-KMS, vous devez fournir une clé KMS gérée par le client dans la même région que votre bucket à usage général. Vous pouvez définir le type de chiffrement de vos tables uniquement lors de leur création. Une fois qu'une table AWS gérée est créée, vous ne pouvez pas modifier ses paramètres de chiffrement. Pour spécifier SSE-KMS pour vos tables de métadonnées, vous devez disposer de certaines autorisations. Pour plus d'informations, consultez la section Autorisations pour SSE-KMS.

Le paramètre de chiffrement d'une table de métadonnées a priorité sur le paramètre de chiffrement par défaut au niveau du compartiment. Si vous ne spécifiez pas de chiffrement pour une table, celle-ci héritera du paramètre de chiffrement par défaut du compartiment.

AWS les compartiments de tables gérés ne sont pas pris en compte dans vos quotas de tables S3. Pour plus d'informations sur l'utilisation des compartiments de tables AWS gérés et des tables AWS gérées, consultez la section Utilisation des compartiments de tables AWS gérés.

Pour surveiller les mises à jour apportées à la configuration de votre table de métadonnées, vous pouvez utiliser AWS CloudTrail. Pour de plus amples informations, veuillez consulter the section called “Actions au niveau du compartiment Amazon S3 suivies par journalisation CloudTrail ”.

Maintenance des tables de métadonnées et expiration des enregistrements

Pour optimiser les performances de vos tables de métadonnées , Amazon S3 effectue des activités de maintenance périodiques sur ces tables, telles que le compactage et la suppression des fichiers non référencés. Ces activités de maintenance permettent à la fois de minimiser le coût de stockage de vos tables de métadonnées et d'optimiser les performances des requêtes. Cette maintenance des tables se fait automatiquement. Elle ne nécessite aucune activation ni aucune gestion continue de votre part.

> **Note**
>
> - Vous ne pouvez pas contrôler l'expiration des instantanés de la table de journal ou de la table d'inventaire. Pour chaque table, Amazon S3 stocke au moins un instantané pendant 24 heures au maximum.
> - Pour réduire vos coûts, vous pouvez configurer l'expiration des enregistrements de la table de journal. Par défaut, les enregistrements de table de journal n'expirent pas et les enregistrements de table de journal doivent être conservés pendant au moins 7 jours. Pour de plus amples informations, veuillez consulter the section called “Enregistrements de table de journal expirant”.

Rubriques

- Limites et restrictions liées à une table de métadonnées
- Schéma des tables de journal des métadonnées S3
- Schéma des tables d'inventaire en temps réel des métadonnées S3
- Configuration des tables de métadonnées
- Interrogation des tables de métadonnées
- Résolution des problèmes liés aux métadonnées S3

Limites et restrictions liées à une table de métadonnées

Les métadonnées Amazon S3 sont soumises aux limites et restrictions suivantes :

- Les métadonnées S3 ne sont actuellement disponibles que dans les régions USA Est (Virginie du Nord), USA Est (Ohio) et USA Ouest (Oregon).
- S3 Metadata prend en charge toutes les classes de stockage prises en charge par les buckets à usage général. Pour la classe de stockage S3 Intelligent-Tiering, le niveau spécifique n'est pas affiché dans la table de métadonnées.
- Lorsque vous créez une configuration de table de métadonnées, vos tables de métadonnées sont stockées dans un bucket de tables AWS géré. Vous ne pouvez pas stocker votre configuration dans un bucket de table géré par le client.
- Les métadonnées S3 ne sont pas prises en charge pour les compartiments de répertoire, les compartiments de table ou les compartiments vectoriels. Vous pouvez créer des configurations de table de métadonnées uniquement pour des compartiments à usage général. La table de journal capture les métadonnées uniquement pour les événements de modification (tels que les téléchargements, les mises à jour et les suppressions) qui se produisent après que vous avez créé la configuration de votre table de métadonnées.
- Vous ne pouvez pas contrôler l'expiration des instantanés de la table de journal ou de la table d'inventaire. Pour chaque table, Amazon S3 stocke au moins un instantané pendant 24 heures au maximum.

  Pour réduire vos coûts, vous pouvez configurer l'expiration des enregistrements de la table de journal. Par défaut, les enregistrements de table de journal n'expirent pas et les enregistrements de table de journal doivent être conservés pendant au moins 7 jours. Pour de plus amples informations, veuillez consulter the section called “Enregistrements de table de journal expirant”.

- Vous ne pouvez créer une configuration de table de métadonnées que pour un compartiment complet à usage général. Vous ne pouvez pas appliquer de configuration de table de métadonnées au niveau du préfixe.
- Vous ne pouvez pas suspendre et reprendre les mises à jour des tables de métadonnées. Vous pouvez toutefois supprimer la configuration de métadonnées associée pour les journaux ou les tables d'inventaire dynamiques. La suppression de votre configuration n'entraîne pas la suppression du journal ou de la table d'inventaire associés. Pour recréer votre configuration, vous devez d'abord supprimer l'ancien journal ou table d'inventaire, puis Amazon S3 peut créer un nouveau journal ou une nouvelle table d'inventaire. Lorsque vous réactivez le tableau d'inventaire, Amazon S3 crée un nouveau tableau d'inventaire et vous êtes à nouveau facturé pour le remplissage du nouveau tableau d'inventaire.
- Les tables de métadonnées ne contiennent pas toutes les mêmes métadonnées que celles disponibles via l'inventaire S3 ou l'API REST Amazon S3. Par exemple, les informations suivantes ne sont pas disponibles dans les tables de métadonnées :
  - Expiration, éligibilité ou statut de transition du cycle de vie S3
  - Période de rétention ou mode de gouvernance du verrouillage d'objet
  - Informations relatives à la liste de contrôle d'accès (ACL) des objets
  - Statut de réplication
- Lorsque vous utilisez Amazon Athena ou Amazon Redshift pour interroger vos tables de métadonnées, vous devez placer les noms des espaces de noms de vos tables de métadonnées entre guillemets " () ou backticks ` (), sinon la requête risque de ne pas fonctionner. Pour obtenir des exemples, consultez the section called "Exemples de requêtes de tables de métadonnées".
- Lorsque vous utilisez Apache Spark Amazon EMR ou d'autres moteurs tiers pour interroger vos tables de métadonnées, nous vous recommandons d'utiliser le point de terminaison Iceberg REST Amazon S3 Tables. Votre requête risque de ne pas s'exécuter correctement si vous n'utilisez pas ce point de terminaison. Pour de plus amples informations, veuillez consulter the section called "Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison".

Schéma des tables de journal des métadonnées S3

Le tableau du journal enregistre les modifications apportées à vos données en temps quasi réel, ce qui vous aide à identifier les nouvelles données téléchargées dans votre bucket, à suivre les objets récemment supprimés, à surveiller les transitions du cycle de vie, etc. La table du journal enregistre les nouveaux objets et les mises à jour de vos objets et de leurs métadonnées (mises à jour nécessitant une opération PUT ou une DELETE opération). Comme cette table peut être

interrogée, vous pouvez auditer les modifications apportées à votre bucket par le biais de simples requêtes SQL.

Vous pouvez utiliser le tableau du journal pour les cas d'utilisation liés à la sécurité, à l'audit et à la conformité afin de suivre les objets chargés, supprimés et modifiés dans le compartiment. Par exemple, vous pouvez interroger le tableau du journal pour répondre à des questions telles que :

- Quels objets ont été supprimés au cours des dernières 24 heures par S3 Lifecycle ?
- De quelles adresses IP proviennent les PUT demandes les plus récentes ?
- Quelles AWS Key Management Service (AWS KMS) clés ont été utilisées pour les PUT demandes au cours des 7 derniers jours ?
- Quels objets de votre bucket ont été créés par Amazon Bedrock au cours des cinq derniers jours ?

Les tables de journal des métadonnées Amazon S3 contiennent des lignes et des colonnes. Chaque ligne représente un événement de mutation qui a créé, mis à jour ou supprimé un objet dans votre compartiment à usage général. La plupart de ces événements sont le résultat d'actions de l'utilisateur, mais certains d'entre eux sont le résultat d'actions entreprises par Amazon S3 en votre nom, telles que l'expiration du cycle de vie de S3 ou les transitions de classes de stockage.

Les tables de journal des métadonnées S3 sont finalement cohérentes avec les modifications survenues dans votre compartiment à usage général. Dans certains cas, au moment où S3 Metadata est informée de la création ou de la mise à jour d'un objet, cet objet a peut-être déjà été remplacé ou supprimé dans le compartiment. Dans de tels cas, les objets ne peuvent plus être récupérés et certaines colonnes peuvent afficher une valeur NULL pour indiquer un schéma de métadonnées manquant.

Voici un exemple de table de journal pour un compartiment à usage général nommé `amzn-s3-demo-bucket`:

```
bucket               key                         sequence_number
                                                                    record_type
 record_timestamp          version_id   is_delete_marker   size   last_modified_date
   e_tag                           storage_class  is_multipart   encryption_status
 is_bucket_key_enabled   kms_key_arn
                checksum_algorithm   object_tags   user_metadata

    requester      source_ip_address   request_id
amzn-s3-demo-bucket Finance/statement1.pdf
 80e737d8b4d82f776affffffffffffff006737d8b4d82f776a00000000000000000000000000000000000000000000
```

```
   CREATE        2024-11-15 23:26:44.899                 FALSE
 6223   11/15/2024 23:26     e131b86632dda753aac4018f72192b83    STANDARD
 FALSE          SSE-KMS             FALSE                   arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890df   SSECRC32             {}
            {count -> Asia, customs -> false, family -> true, location -> Mary, name ->
 football, user -> United States}                      111122223333   192.0.2.1
    CVK8FWYRW0M9JW65
amzn-s3-demo-bucket s3-dg.pdf
 80e737d8b4e39f1dbdfffffffffffffff006737d8b4e39f1dbd000000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.942                 FALSE
 3554   11/15/2024 23:26     9bb49efc2d92c05558ddffbbde8636d5    STANDARD
 FALSE          DSSE-KMS            FALSE                   arn:aws:kms:us-
east-1:936810216292:key/0dcebce6-49fd-4cae-b2e2-5512ad281afd   SSESHA1              {}
           {}
                                                    111122223333   192.0.2.1
   CVKAQDRAZEG7KXAY
amzn-s3-demo-bucket Development/Projects.xls
 80e737d8b4ed9ac5c6fffffffffffffff006737d8b4ed9ac5c600000000000000000000000000000000000000000000000
   CREATE        2024-11-15 23:26:44.966                 FALSE              7746
 11/15/2024 23:26     729a6863e47fb9955b31bfabce984908    STANDARD   FALSE
 SSE-S3              FALSE                   NULL
                                  SSECRC32             {}            {count -> Asia,
 customs -> Canada, family -> Billiards, filter -> true, location -> Europe, name ->
 Asia, user -> United States}   111122223333   192.0.2.1           CVK7Z6XQTQ90BSRV
```

Les tables de journaux présentent le schéma suivant :

Nom de la colonne	Obligatoire ?	Type de données	
`bucket`	Oui	Chaîne	Nom du compartiment à usage général. Pour de plus amples informations, veuillez consulter the section called “Règles de dénomination”.
`key`	Oui	Chaîne	Nom de la clé d'objet (ou clé) qui identifie de manière unique l'objet dans

Nom de la colonne	Obligatoire ?	Type de données	
			le compartiment. Pour de plus amples informations, veuillez consulter the section called "Attribution d'un nom aux objets".
`sequence_number`	Oui	Chaîne	Numéro de séquence, qui est un ordinal inclus dans les enregistrements d'un objet donné. Pour ordonner des enregistrements contenant le même compartiment et la même clé, vous pouvez effectuer un tri par `sequence_number`. Pour un compartiment et une clé donnés, une valeur `sequence_number` plus élevée du point de vue lexicographique signifie que l'enregistrement a été introduit dans le compartiment plus récemment.

Nom de la colonne	Obligatoire ?	Type de données	
`record_type`	Oui	Chaîne	Type de cet enregistrement : `CREATE`, `UPDATE_METADATA` ou `DELETE`. Les enregistrements `CREATE` indiquent qu'un nouvel objet (ou une nouvelle version de l'objet) a été écrit dans le compartiment. Les enregistrements `UPDATE_METADATA` capturent les modifications apportées aux métadonnées mutables d'un objet existant, telles que la classe de stockage ou les balises. Les enregistrements `DELETE` indiquent que cet objet (ou cette version de l'objet) a été supprimé. Lorsque la gestion des versions est activée, les enregistrements `DELETE` représentent soit un marqueur de suppression, soit une

Nom de la colonne	Obligatoire ?	Type de données	
			suppression définitive. Les marqueurs de suppression ont une valeur `record_type` correspondant à `DELETE` et une valeur `is_delete_marker` correspondant à `True`. Les enregistrements de suppression définitive ont des valeurs nulles dans toutes les autres colonnes, à l'exception de `bucket`, `key`, `sequence_number`, `record_type`, `record_timestamp` et `version_id`. Pour de plus amples informations, veuillez consulter the section called "Suppression des versions d'objet".
`record_timestamp`	Oui	Horodatage NTZ (sans fuseau horaire)	Horodatage associé à cet enregistrement.

Nom de la colonne	Obligatoire ?	Type de données	
`version_id`	Non	Chaîne	ID de version de l'objet. Lorsque vous activez la gestion des versions sur un compartiment, Amazon S3 attribue un numéro de version aux objets qui sont ajoutés au compartiment. Pour de plus amples informations, veuillez consulter the section called "Conservation de plusieurs versions d'objets". Les objets qui sont stockés dans le compartiment avant que vous définissiez l'état de la gestion des versions ont un ID de version nul.

Nom de la colonne	Obligatoire ?	Type de données	
`is_delete_marker`	Non	Booléen	Statut du marqueur de suppression de l'objet. Si l'objet est un marqueur de suppression, cette valeur est `True`. Sinon, la valeur est définie comme `False`. Pour de plus amples informations, veuillez consulter the section called "Utilisation des marqueurs de suppression". **Note** Les lignes ajoutées pour les marqueurs de suppression ont une valeur `record_type` correspondant à `DELETE`, pas à `UPDATE_METADATA` . Si le marqueur de suppression est créé à la suite de l'expiration du

Nom de la colonne	Obligatoire ?	Type de données	
			cycle de vie S3, la valeur `requester` est `s3.amazonaws.com` .
`size`	Non	Long	Taille de l'objet en octets, à l'exclusion de la taille des chargements partitionnés incomplets, ou des métadonnées de l'objet. Si `is_delete_marker` correspond à `True`, la taille est `0`. Pour de plus amples informations, veuillez consulter the section called "Métadonnées d'objet définies par le système".

Nom de la colonne	Obligatoire ?	Type de données	
`last_modified_date`	Non	Horodatage NTZ (sans fuseau horaire)	La date de création ou de dernière modification, la plus récente des deux. Pour les chargements partitionnés, la date de création de l'objet correspond à la date de lancement du chargement partitionné. Pour de plus amples informations, veuillez consulter the section called "Métadonnées d'objet définies par le système".

Nom de la colonne	Obligatoire ?	Type de données	
`e_tag`	Non	Chaîne	La balise d'entité (ETag), qui est un hachage de l'objet. Le ETag reflète les modifications apportées uniquement au contenu d'un objet, et non à ses métadonnées. Il ETag peut s'agir d'un MD5 condensé des données de l'objet. La question de savoir s'il s' ETag agit d'un MD5 condensé dépend de la manière dont l'objet a été créé et de son cryptage. Pour plus d'informations, consultez Object dans la Référence d'API Amazon S3.

Nom de la colonne	Obligatoire ?	Type de données	
`storage_class`	Non	Chaîne	Classe de stockage utilisée pour stocker l'objet. `STANDARD`, `REDUCED_REDUNDANCY`, `STANDARD_IA`, `ONEZONE_IA`, `INTELLIGENT_TIERING`, `GLACIER`, `DEEP_ARCHIVE`, ou `GLACIER_IR`. Pour de plus amples informations, veuillez consulter the section called "Bien comprendre et gérer les classes de stockage".
`is_multipart`	Non	Booléen	Type de chargement de l'objet. Si l'objet a été chargé dans un chargement partitionné, cette valeur est `True`. Sinon, la valeur est définie comme `False`. Pour de plus amples informations, veuillez consulter the section called "Utilisation du chargement partitionné".

Nom de la colonne	Obligatoire ?	Type de données	
`encryption_status`	Non	Chaîne	Statut du chiffrement côté serveur de l'objet, en fonction du type de clé de chiffrement utilisé : chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3), chiffrement côté serveur avec les clés AWS Key Management Service (AWS KMS) (SSE-KMS), chiffrement double couche côté serveur avec AWS KMS keys (DSSE-KMS) ou chiffrement côté serveur avec les clés fournies par le client (SSE-C). Si l'objet n'est pas chiffré, la valeur est nulle. Les valeurs possibles sont `SSE-S3`, `SSE-KMS`, `DSSE-KMS`, `SSE-C` ou « null ». Pour de plus amples informations, veuillez consulter the section called "Chiffrement des données".

Nom de la colonne	Obligatoire ?	Type de données	
`is_bucket_key_enabled`	Non	Booléen	Statut d'activation de la clé de compartiment S3 de l'objet. Si l'objet utilise une clé de compartiment S3 pour SSE-KMS, cette valeur est `True`. Sinon, la valeur est définie comme `False`. Pour de plus amples informations, veuillez consulter the section called "Configuration d'une clé de compartiment S3 pour un objet".

Nom de la colonne	Obligatoire ?	Type de données	
`kms_key_arn`	Non	Chaîne	Amazon Resource Name (ARN) de la clé KMS avec laquelle l'objet est chiffré, pour les lignes où `encryption_status` correspond à `SSE-KMS` ou `DSSE-KMS`. Si l'objet n'est pas chiffré avec SSE-KMS ou DSSE-KMS, la valeur est nulle. Pour plus d'informations, consultez the section called "Clés KMS stockées dans AWS KMS (SSE-KMS)" et the section called "Chiffrement double couche côté serveur (DSSE-KMS)". **Note** Si une ligne représente une version d'objet qui n'existait plus au moment du traitement d'un événement de suppressi

Nom de la colonne	Obligatoire ?	Type de données	
			on ou de remplacement, `kms_key_arn` contient une valeur nulle, même si la valeur de la colonne `encryption_status` indique `SSE-KMS` ou `DSSE-KMS`.
`checksum_algorithm`	Non	Chaîne	Algorithme utilisé pour créer la somme de contrôle pour l'objet : `CRC64NVME` , `CRC32`, `CRC32C`, `SHA1` ou `SHA256`. Si aucune somme de contrôle n'est présente, cette valeur est nulle. Pour de plus amples informations, veuillez consulter the section called "Utilisation des algorithmes de total de contrôle pris en charge".

Nom de la colonne	Obligatoire ?	Type de données	
`object_tags`	Non	Map <String, String>	Balises associées à l'objet. Les balises d'objets sont stockées sous forme de mappage de paires clé-valeur. Si un objet ne possède aucune balise, un mappage vide (`{}`) est stocké. Pour de plus amples informations, veuillez consulter the section called "Catégorisation des objets à l'aide de balises". **Note** Si la valeur `record_type` indique `DELETE`, la colonne `object_tags` contient une valeur nulle. Si la valeur `record_type` indique `CREATE` ou `UPDATE_METADATA`, les lignes représentant

Nom de la colonne	Obligatoire ?	Type de données	
			des versions d'objets qui n'existaient plus au moment du traitement d'un événement de suppression ou de remplacement contenant une valeur nulle dans la colonne `object_tags` .

Nom de la colonne	Obligatoire ?	Type de données	
`user_metadata`	Non	Map <String, String>	Métadonnées utilisateur associées à l'objet. Les métadonnées utilisateur sont stockées sous forme de mappage de paires clé-valeur. Si un objet ne possède aucune métadonnée utilisateur, un mappage vide (`{}`) est stocké. Pour de plus amples informations, veuillez consulter the section called "Métadonnées d'objet définies par l'utilisateur". **Note** Si la valeur `record_type` indique `DELETE`, la colonne `user_metadata` contient une valeur nulle. Si la valeur `record_type` indique `CREATE` ou `UPDATE_METADATA` ,

Nom de la colonne	Obligatoire ?	Type de données	
			les lignes représentant des versions d'objets qui n'existaient plus au moment du traitement d'un événement de suppression ou de remplacement contiennent une valeur nulle dans la colonne `user_metadata` .
`requester`	Non	Chaîne	L' Compte AWS ID du demandeur ou du Service AWS principal auteur de la demande. Par exemple, si le demandeur est S3 Lifecycle, cette valeur est `s3.amazonaws.com` .

Nom de la colonne	Obligatoire ?	Type de données	
`source_ip_address`	Non	Chaîne	Adresse IP source de la demande. Pour les enregistrements générés par une demande utilisateur, cette colonne contient l'adresse IP source de la demande. Pour les actions entreprises par Amazon S3 ou une autre entité Service AWS au nom de l'utilisateur, cette colonne contient une valeur nulle.
`request_id`	Non	Chaîne	ID associé à la demande.

Schéma des tables d'inventaire en temps réel des métadonnées S3

Le tableau d'inventaire en temps réel fournit un inventaire simple et interrogeable de tous les objets et de leurs versions dans votre compartiment afin que vous puissiez déterminer l'état le plus récent de vos données. Les mises à jour de vos objets sont généralement reflétées dans le tableau d'inventaire dans un délai d'une heure.

Vous pouvez utiliser ce tableau pour simplifier et accélérer les flux de travail métier et les tâches liées au Big Data en identifiant les objets que vous souhaitez traiter pour différentes charges de travail. Par exemple, vous pouvez interroger la table d'inventaire pour effectuer les opérations suivantes :

- Trouvez tous les objets stockés dans la classe de stockage S3 Glacier Deep Archive.
- Créez une distribution de balises d'objets ou recherchez des objets sans balises.
- Trouvez tous les objets qui ne sont pas chiffrés à l'aide du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS).

Lorsque vous activez la table d'inventaire pour la configuration de votre table de métadonnées, la table est soumise à un processus appelé backfilling, au cours duquel Amazon S3 analyse votre compartiment à usage général pour récupérer les métadonnées initiales de tous les objets du compartiment. Selon le nombre d'objets contenus dans votre compartiment, ce processus peut prendre de quelques minutes (minimum 15 minutes) à plusieurs heures. Lorsque le processus de remblayage est terminé, le statut de votre tableau d'inventaire passe de Remblayage à Actif. Une fois le remblayage terminé, les mises à jour apportées à vos objets sont généralement reflétées dans le tableau d'inventaire en moins d'une heure.

> **Note**
>
> Le remplissage de votre tableau d'inventaire vous est facturé. Si votre bucket à usage général contient plus d'un milliard d'objets, des frais mensuels vous sont également facturés pour votre tableau d'inventaire. Pour plus d'informations, consultez Tarification Amazon S3.

Les tables d'inventaire des métadonnées Amazon S3 contiennent des lignes et des colonnes. Chaque ligne représente l'état actuel d'un objet dans votre compartiment à usage général. Le tableau d'inventaire fournit un inventaire simple et interrogeable de tous les objets de votre compartiment afin que vous puissiez déterminer l'état actuel de vos données.

Voici un exemple de table d'inventaire pour un compartiment à usage général nommé `amzn-s3-demo-bucket:`

```
bucket               key                         sequence_number
                                                                    version_id
   is_delete_marker   size   last_modified_date   e_tag
 storage_class   is_multipart   encryption_status   is_bucket_key_enabled   kms_key_arn
                                                              checksum_algorithm
 object_tags   user_metadata
amzn-s3-demo-bucket Finance/statement1.pdf
 80e737d8b4d82f776affffffffffffff006737d8b4d82f776a00000000000000000000000000000000000000000000
               FALSE             6223   11/15/2024 23:26
  e131b86632dda753aac4018f72192b83    STANDARD   FALSE
   SSE-KMS             FALSE                   arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890df   SSECRC32             {}
            {count -> Asia, customs -> false, family -> true, location -> Mary, name ->
 football, user -> United States}
amzn-s3-demo-bucket s3-dg.pdf
 80e737d8b4e39f1dbdffffffffffffff006737d8b4e39f1dbd00000000000000000000000000000000000000000000
```

```
                FALSE              3554   11/15/2024 23:26
 9bb49efc2d92c05558ddffbbde8636d5    STANDARD   FALSE          DSSE-KMS
 FALSE                   arn:aws:kms:us-east-1:936810216292:key/0dcebce6-49fd-4cae-
b2e2-5512ad281afd   SSESHA1              {}            {}
amzn-s3-demo-bucket Development/Projects.xls
 80e737d8b4ed9ac5c6fffffffffffffff006737d8b4ed9ac5c60000000000000000000000000000000000000000
                FALSE              7746   11/15/2024 23:26
 729a6863e47fb9955b31bfabce984908    STANDARD   FALSE          SSE-S3
 FALSE                   NULL
                SSECRC32             {}            {count -> Asia, customs -> Canada,
 family -> Billiards, filter -> true, location -> Europe, name -> Asia, user -> United
 States}
```

Les tables d'inventaire présentent le schéma suivant :

Nom de la colonne	Obligatoire ?	Type de données	
`bucket`	Oui	Chaîne	Nom du compartiment à usage général. Pour de plus amples informations, veuillez consulter the section called “Règles de dénomination”.
`key`	Oui	Chaîne	Nom de la clé d'objet (ou clé) qui identifie de manière unique l'objet dans le compartiment. Pour de plus amples informations, veuillez consulter the section called “Attribution d'un nom aux objets”.
`sequence_number`	Oui	Chaîne	Numéro de séquence, qui est un ordinal inclus dans les

Nom de la colonne	Obligatoire ?	Type de données	
			enregistrements d'un objet donné. Pour ordonner des enregistrements contenant le même compartiment et la même clé, vous pouvez effectuer un tri par `sequence_number` . Pour un compartiment et une clé donnés, une valeur `sequence_number` plus élevée du point de vue lexicographique signifie que l'enregistrement a été introduit dans le compartiment plus récemment.

Nom de la colonne	Obligatoire ?	Type de données	
`version_id`	Non	Chaîne	ID de version de l'objet. Lorsque vous activez la gestion des versions sur un compartiment, Amazon S3 attribue un numéro de version aux objets qui sont ajoutés au compartiment. Pour de plus amples informations, veuillez consulter the section called "Conservation de plusieurs versions d'objets". Les objets qui sont stockés dans le compartiment avant que vous définissiez l'état de la gestion des versions ont un ID de version nul.

Nom de la colonne	Obligatoire ?	Type de données	
`is_delete_marker`	Non	Booléen	Statut du marqueur de suppression de l'objet. Si l'objet est un marqueur de suppression, cette valeur est `True`. Sinon, la valeur est définie comme `False`. Pour de plus amples informations, veuillez consulter the section called "Utilisation des marqueurs de suppression". **Note** Les lignes ajoutées pour les marqueurs de suppression ont une valeur `record_type` correspondant à `DELETE`, pas à `UPDATE_METADATA`. Si le marqueur de suppression est créé à la suite de l'expiration du

Nom de la colonne	Obligatoire ?	Type de données	
			cycle de vie S3, la valeur `requester` est `s3.amazonaws.com` .
`size`	Non	Long	Taille de l'objet en octets, à l'exclusion de la taille des chargements partitionnés incomplets, ou des métadonnées de l'objet. Si `is_delete_marker` correspond à `True`, la taille est `0`. Pour de plus amples informations, veuillez consulter the section called "Métadonnées d'objet définies par le système".

Nom de la colonne	Obligatoire ?	Type de données	
`last_modified_date`	Non	Horodatage NTZ (sans fuseau horaire)	La date de création ou de dernière modification, la plus récente des deux. Pour les chargements partitionnés, la date de création de l'objet correspond à la date de lancement du chargement partitionné. Pour de plus amples informations, veuillez consulter the section called "Métadonnées d'objet définies par le système".

Nom de la colonne	Obligatoire ?	Type de données	
`e_tag`	Non	Chaîne	La balise d'entité (ETag), qui est un hachage de l'objet. Le ETag reflète les modifications apportées uniquement au contenu d'un objet, et non à ses métadonnées. Il ETag peut s'agir d'un MD5 condensé des données de l'objet. La question de savoir s'il s' ETag agit d'un MD5 condensé dépend de la manière dont l'objet a été créé et de son cryptage. Pour plus d'informations, consultez Object dans la Référence d'API Amazon S3.

Nom de la colonne	Obligatoire ?	Type de données	
`storage_class`	Non	Chaîne	Classe de stockage utilisée pour stocker l'objet. `STANDARD`, `REDUCED_REDUNDANCY`, `STANDARD_IA`, `ONEZONE_IA`, `INTELLIGENT_TIERING`, `GLACIER`, `DEEP_ARCHIVE`, ou `GLACIER_IR`. Pour de plus amples informations, veuillez consulter the section called "Bien comprendre et gérer les classes de stockage".
`is_multipart`	Non	Booléen	Type de chargement de l'objet. Si l'objet a été chargé dans un chargement partitionné, cette valeur est `True`. Sinon, la valeur est définie comme `False`. Pour de plus amples informations, veuillez consulter the section called "Utilisation du chargement partitionné".

Nom de la colonne	Obligatoire ?	Type de données	
`encryption_status`	Non	Chaîne	Statut du chiffrement côté serveur de l'objet, en fonction du type de clé de chiffrement utilisé : chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3), chiffrement côté serveur avec les clés AWS Key Management Service (AWS KMS) (SSE-KMS), chiffrement double couche côté serveur avec AWS KMS keys (DSSE-KMS) ou chiffrement côté serveur avec les clés fournies par le client (SSE-C). Si l'objet n'est pas chiffré, la valeur est nulle. Les valeurs possibles sont `SSE-S3`, `SSE-KMS`, `DSSE-KMS`, `SSE-C` ou « null ». Pour de plus amples informations, veuillez consulter the section called "Chiffrement des données".

Nom de la colonne	Obligatoire ?	Type de données	
`is_bucket_key_enabled`	Non	Booléen	Statut d'activation de la clé de compartiment S3 de l'objet. Si l'objet utilise une clé de compartiment S3 pour SSE-KMS, cette valeur est `True`. Sinon, la valeur est définie comme `False`. Pour de plus amples informations, veuillez consulter the section called "Configuration d'une clé de compartiment S3 pour un objet".

Nom de la colonne	Obligatoire ?	Type de données	
`kms_key_arn`	Non	Chaîne	Amazon Resource Name (ARN) de la clé KMS avec laquelle l'objet est chiffré, pour les lignes où `encryption_status` correspond à `SSE-KMS` ou `DSSE-KMS`. Si l'objet n'est pas chiffré avec SSE-KMS ou DSSE-KMS, la valeur est nulle. Pour plus d'informations, consultez the section called "Clés KMS stockées dans AWS KMS (SSE-KMS)" et the section called "Chiffrement double couche côté serveur (DSSE-KMS)". **Note** Si une ligne représente une version d'objet qui n'existait plus au moment du traitement d'un événement de suppressi

Nom de la colonne	Obligatoire ?	Type de données	
			on ou de remplacement, `kms_key_arn` contient une valeur nulle, même si la valeur de la colonne `encryption_status` indique `SSE-KMS` ou `DSSE-KMS`.
`checksum_algorithm`	Non	Chaîne	Algorithme utilisé pour créer la somme de contrôle pour l'objet : `CRC64-NVME`, `CRC32`, `CRC32C`, `SHA1` ou `SHA256`. Si aucune somme de contrôle n'est présente, cette valeur est nulle. Pour de plus amples informations, veuillez consulter the section called "Utilisation des algorithmes de total de contrôle pris en charge".

Nom de la colonne	Obligatoire ?	Type de données	
`object_tags`	Non	Map <String, String>	Balises associées à l'objet. Les balises d'objets sont stockées sous forme de mappage de paires clé-valeur. Si un objet ne possède aucune balise, un mappage vide (`{}`) est stocké. Pour de plus amples informations, veuillez consulter the section called "Catégorisation des objets à l'aide de balises". **Note** Si la valeur `record_type` indique `DELETE`, la colonne `object_tags` contient une valeur nulle. Si la valeur `record_type` indique `CREATE` ou `UPDATE_METADATA`, les lignes représentant

Nom de la colonne	Obligatoire ?	Type de données	
			des versions d'objets qui n'existaient plus au moment du traitement d'un événement de suppression ou de remplacement contenant une valeur nulle dans la colonne `object_tags` .

Nom de la colonne	Obligatoire ?	Type de données	
`user_metadata`	Non	Map <String, String>	Métadonnées utilisateur associées à l'objet. Les métadonnées utilisateur sont stockées sous forme de mappage de paires clé-valeur. Si un objet ne possède aucune métadonnée utilisateur, un mappage vide (`{}`) est stocké. Pour de plus amples informations, veuillez consulter the section called "Métadonnées d'objet définies par l'utilisateur". **Note** Si la valeur `record_type` indique `DELETE`, la colonne `user_metadata` contient une valeur nulle. Si la valeur `record_type` indique `CREATE` ou `UPDATE_METADATA` ,

Nom de la colonne	Obligatoire ?	Type de données	
			les lignes représentant des versions d'objets qui n'existaient plus au moment du traitement d'un événement de suppression ou de remplacement contiennent une valeur nulle dans la colonne `user_metadata`.

Configuration des tables de métadonnées

Les métadonnées Amazon S3 accélèrent la découverte des données en capturant automatiquement les métadonnées des objets de vos compartiments à usage général et en les stockant dans des tables Apache Iceberg entièrement gérées en lecture seule que vous pouvez interroger. Ces tables en lecture seule sont appelées tables de métadonnées. Lorsque des objets sont ajoutés, mis à jour ou supprimés dans vos compartiments à usage général, les métadonnées S3 actualisent automatiquement les tables de métadonnées correspondantes pour refléter les dernières modifications.

Avec les métadonnées S3, vous pouvez facilement rechercher, stocker et interroger les métadonnées de vos objets S3, afin de préparer rapidement les données à utiliser dans l'analytique métier, l'entraînement des modèles d'intelligence artificielle et de machine learning (IA/ML), etc.

Pour générer et stocker des métadonnées d'objets dans des tables de métadonnées AWS gérées, vous devez créer une configuration de table de métadonnées pour votre bucket à usage général. Amazon S3 est conçu pour mettre à jour en permanence les tables de métadonnées afin de refléter les dernières modifications apportées à vos données tant que la configuration est active sur le compartiment. En outre, Amazon S3 optimise en permanence vos tables de métadonnées afin de réduire les coûts de stockage et d'améliorer les performances des requêtes d'analytique.

Pour créer une configuration de table de métadonnées, assurez-vous que vous disposez des autorisations AWS Identity and Access Management (IAM) nécessaires pour créer et gérer des tables de métadonnées.

Pour surveiller les mises à jour apportées à la configuration de votre table de métadonnées, vous pouvez utiliser AWS CloudTrail. Pour de plus amples informations, veuillez consulter the section called "Actions au niveau du compartiment Amazon S3 suivies par journalisation CloudTrail ".

Rubriques

- Définition des autorisations pour la configuration des tables de métadonnées
- Création de configurations de tables de métadonnées
- Contrôle de l'accès aux tables de métadonnées
- Enregistrements de table de journal expirant
- Activation ou désactivation des tables d'inventaire dynamiques
- Afficher les configurations des tables de métadonnées
- Suppression de configurations de tables de métadonnées
- Suppression des tables de métadonnées

Définition des autorisations pour la configuration des tables de métadonnées

Pour créer une configuration de table de métadonnées, vous devez disposer des autorisations AWS Identity and Access Management (IAM) nécessaires à la fois pour créer et gérer la configuration de votre table de métadonnées et pour créer et gérer vos tables de métadonnées et le compartiment de tables dans lequel vos tables de métadonnées sont stockées.

Pour créer et gérer la configuration de votre table de métadonnées, vous devez disposer des autorisations suivantes :

- `s3:CreateBucketMetadataTableConfiguration` : cette autorisation vous permet de créer une configuration de table de métadonnées pour votre compartiment à usage général. Pour créer

une configuration de table de métadonnées, des autorisations supplémentaires, notamment des autorisations S3 Tables, sont requises, comme expliqué dans les sections suivantes. Pour un résumé des autorisations requises, consultezthe section called "Opérations de compartiment et autorisations".

- `s3:GetBucketMetadataTableConfiguration` : cette autorisation vous permet d'extraire les informations relatives à la configuration de votre table de métadonnées.
- `s3:DeleteBucketMetadataTableConfiguration` : cette autorisation vous permet de supprimer les informations relatives à la configuration de votre table de métadonnées.
- `s3:UpdateBucketMetadataJournalTableConfiguration`— Cette autorisation vous permet de mettre à jour la configuration de votre table de journal pour faire expirer les enregistrements de la table de journal.
- `s3:UpdateBucketMetadataInventoryTableConfiguration`— Cette autorisation vous permet de mettre à jour la configuration de votre table d'inventaire pour activer ou désactiver la table d'inventaire. Pour mettre à jour la configuration d'une table d'inventaire, des autorisations supplémentaires, notamment des autorisations S3 Tables, sont requises. Pour obtenir la liste des autorisations requises, consultez the section called "Opérations de compartiment et autorisations".

> **Note**
>
> Les `s3:DeleteBucketMetadataTableConfiguration` autorisations `s3:CreateBucketMetadataTableConfigurations3:GetBucketMetadataTableConfigur` et sont utilisées pour les configurations de métadonnées S3 V1 et V2. Pour la V2, les noms des opérations d'API correspondantes sont `CreateBucketMetadataConfigurationGetBucketMetadataConfiguration`, et`DeleteBucketMetadataConfiguration`.

Pour créer et gérer des tables et des compartiments de tables, vous devez disposer de certaines autorisations `s3tables`. Au minimum, pour créer une configuration de table de métadonnées, vous devez disposer des autorisations `s3tables` suivantes :

- `s3tables:CreateTableBucket`— Cette autorisation vous permet de créer un bucket de table AWS géré. Toutes les configurations de tables de métadonnées de votre compte et de la même région sont stockées dans un seul compartiment de table AWS géré nommé`aws-s3`. Pour plus d'informations, reportez-vous à the section called "Fonctionnement des tables de métadonnées" la section Utilisation des compartiments de tables AWS gérés.

- `s3tables:CreateNamespace` : cette autorisation vous permet de créer un espace de noms dans un compartiment de tables. Les tables de métadonnées utilisent généralement l'espace de b*`_general_purpose_bucket_name`* noms. Pour plus d'informations sur les espaces de noms des tables de métadonnées, consultezthe section called “Fonctionnement des tables de métadonnées”.
- `s3tables:CreateTable`— Cette autorisation vous permet de créer vos tables de métadonnées.
- `s3tables:GetTable`— Cette autorisation vous permet de récupérer des informations sur vos tables de métadonnées.
- `s3tables:PutTablePolicy`— Cette autorisation vous permet d'ajouter ou de mettre à jour vos politiques relatives aux tables de métadonnées.
- `s3tables:PutTableEncryption`— Cette autorisation vous permet de définir le chiffrement côté serveur pour vos tables de métadonnées. Des autorisations supplémentaires sont requises si vous souhaitez chiffrer vos tables de métadonnées à l'aide du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Pour plus d'informations, consultez la section Autorisations pour SSE-KMS.
- `kms:DescribeKey`— Cette autorisation vous permet de récupérer des informations sur une clé KMS.

Pour obtenir des informations détaillées sur toutes les autorisations relatives aux tables et aux compartiments de tables, consultez Gestion des accès pour les tables S3.

> **Important**
>
> Si vous souhaitez également intégrer votre compartiment de tables aux services AWS d'analyse afin de pouvoir interroger votre table de métadonnées, vous avez besoin d'autorisations supplémentaires. Pour plus d'informations, consultez la section Intégration des tables Amazon S3 aux services AWS d'analyse.

Autorisations pour SSE-KMS

Pour chiffrer vos tables de métadonnées à l'aide du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), vous devez disposer d'autorisations supplémentaires.

1. L'utilisateur ou le rôle AWS Identity and Access Management (IAM) a besoin des autorisations suivantes. Vous pouvez accorder ces autorisations à l'aide de la console IAM : https://console.aws.amazon.com/iam/.
   a. `s3tables:PutTableEncryption`pour configurer le chiffrement des tables
   b. `kms:DescribeKey`sur la AWS KMS clé utilisée
2. En ce qui concerne la politique de ressources pour la clé KMS, vous avez besoin des autorisations suivantes. Vous pouvez accorder ces autorisations à l'aide de la AWS KMS console : https://console.aws.amazon.com/kms.
   a. Accordez la `kms:GenerateDataKey` permission à `metadata.s3.amazonaws.com` et`maintenance.s3tables.amazonaws.com`.
   b. Accordez la `kms:Decrypt` permission à `metadata.s3.amazonaws.com` et`maintenance.s3tables.amazonaws.com`.
   c. Accordez `kms:DescribeKey` l'autorisation au AWS principal invocateur.

Outre ces autorisations, assurez-vous que la clé KMS gérée par le client utilisée pour chiffrer les tables existe toujours, qu'elle est active et qu'elle se trouve dans la même région que votre compartiment à usage général.

Exemple de stratégie

Pour créer et utiliser des tables de métadonnées et des compartiments de tables, vous pouvez utiliser l'exemple de politique suivant. Dans cette politique, le compartiment à usage général auquel vous appliquez la configuration de la table de métadonnées est appelé *`amzn-s3-demo-bucket`*. Pour utiliser cette politique, remplacez *`user input placeholders`* par vos propres informations.

Lorsque vous créez la configuration de vos tables de métadonnées, celles-ci sont stockées dans un bucket de tables AWS géré. Toutes les configurations de tables de métadonnées de votre compte et de la même région sont stockées dans un seul compartiment de table AWS géré nommé`aws-s3`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PermissionsToWorkWithMetadataTables",
            "Effect": "Allow",
```

```
            "Action": [
                "s3:CreateBucketMetadataTableConfiguration",
                "s3:GetBucketMetadataTableConfiguration",
                "s3:DeleteBucketMetadataTableConfiguration",
                "s3:UpdateBucketMetadataJournalTableConfiguration",
                "s3:UpdateBucketMetadataInventoryTableConfiguration",
                "s3tables:*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:s3:::bucket/amzn-s3-demo-bucket",
                "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3",
                "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/*"
            ]
        }
    ]
}
```

Pour interroger les tables de métadonnées, vous pouvez utiliser l'exemple de politique suivant. Si vos tables de métadonnées ont été chiffrées avec SSE-KMS, vous aurez besoin de l'`kms:Decrypt`autorisation indiquée. Pour utiliser cette politique, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PermissionsToQueryMetadataTables",
            "Effect": "Allow",
            "Action": [
                "s3tables:GetTable",
                "s3tables:GetTableData",
                "s3tables:GetTableMetadataLocation",
                "kms:Decrypt"
            ],
            "Resource": [
                "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3",
                "arn:aws:s3tables:us-east-1:111122223333:bucket/aws-s3/table/*"
            ]
```

```
        }
    ]
}
```

Création de configurations de tables de métadonnées

Pour générer et stocker les métadonnées Amazon S3 dans des tables de Apache Iceberg métadonnées entièrement gérées, vous devez créer une configuration de table de métadonnées pour votre compartiment à usage général. Amazon S3 est conçu pour mettre à jour en permanence les tables de métadonnées afin de refléter les dernières modifications apportées à vos données tant que la configuration est active sur le compartiment. En outre, Amazon S3 optimise en permanence vos tables de métadonnées afin de réduire les coûts de stockage et d'améliorer les performances des requêtes d'analytique.

Pour chaque compartiment à usage général, vous pouvez créer une configuration de table de métadonnées contenant deux tables de métadonnées complémentaires :

- Table de journal : par défaut, la configuration de votre table de métadonnées contient une table de journal qui capture les événements qui se produisent pour les objets de votre compartiment. Le tableau du journal enregistre les modifications apportées à vos données en temps quasi réel, ce qui vous aide à identifier les nouvelles données téléchargées dans votre bucket, à suivre les objets récemment supprimés, à surveiller les transitions du cycle de vie, etc. La table du journal enregistre les nouveaux objets et les mises à jour de vos objets et de leurs métadonnées (mises à jour nécessitant une opération `PUT` ou une `DELETE` opération).

  La table de journal capture les métadonnées uniquement pour les événements de modification (tels que les téléchargements, les mises à jour et les suppressions) qui se produisent après la création de la configuration de votre table de métadonnées. Comme cette table peut être interrogée, vous pouvez auditer les modifications apportées à votre bucket par le biais de simples requêtes SQL.

  La table de journal est obligatoire pour chaque configuration de table de métadonnées. (Dans la version initiale de S3 Metadata, la table de journal était appelée « table de métadonnées ».)

  Pour plus d'informations sur les données stockées dans les tables de journal, voirthe section called "Schéma des tables de journaux".

  Pour minimiser vos coûts de stockage, vous pouvez choisir d'activer l'expiration des enregistrements de la table de journal. Pour de plus amples informations, veuillez consulter the section called "Enregistrements de table de journal expirant".

- Table d'inventaire dynamique : vous pouvez éventuellement ajouter une table d'inventaire dynamique à la configuration de votre table de métadonnées. Le tableau d'inventaire en temps réel fournit un inventaire simple et interrogeable de tous les objets et de leurs versions dans votre compartiment afin que vous puissiez déterminer l'état le plus récent de vos données.

  Vous pouvez utiliser le tableau d'inventaire en temps réel pour simplifier et accélérer les flux de travail commerciaux et les tâches liées au Big Data en identifiant les objets que vous souhaitez traiter pour différentes charges de travail. Par exemple, vous pouvez interroger la table d'inventaire dynamique pour trouver tous les objets stockés dans une classe de stockage donnée, tous les objets dotés de certaines balises, tous les objets qui ne sont pas chiffrés par chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS), etc.

  Lorsque vous activez la table d'inventaire dynamique pour la configuration de votre table de métadonnées, la table est soumise à un processus appelé backfilling, au cours duquel Amazon S3 analyse votre compartiment à usage général pour récupérer les métadonnées initiales de tous les objets présents dans le compartiment. Selon le nombre d'objets contenus dans votre compartiment, ce processus peut prendre de quelques minutes (minimum 15 minutes) à plusieurs heures. Lorsque le processus de remblayage est terminé, le statut de votre tableau d'inventaire en temps réel passe de Remblayage à Actif. Une fois le remblayage terminé, les mises à jour apportées à vos objets sont généralement reflétées dans le tableau d'inventaire en temps réel en moins d'une heure.

  Le remplissage de votre tableau d'inventaire en ligne vous est facturé. Si votre bucket à usage général contient plus d'un milliard d'objets, des frais mensuels vous sont également facturés pour votre tableau d'inventaire en ligne. Pour plus d'informations, consultez Tarification Amazon S3.

  Pour plus d'informations sur les données stockées dans les tables d'inventaire dynamiques, consultezthe section called “Schéma des tables d'inventaire en temps réel”.

Les tables de métadonnées possèdent le format d'Amazon Resource Name (ARN) suivant :

`arn:aws:s3tables:`*`region-code`*`:`*`account-id`*`:bucket/aws-s3/table/`*`metadata_table_name`*

Les tables de journal portent le nom `journal` et les tables d'inventaire dynamiques portent le nom`inventory`.

Lorsque vous créez la configuration de vos tables de métadonnées, celles-ci sont stockées dans un bucket de tables AWS géré. Toutes les configurations de tables de métadonnées de votre compte et

de la même région sont stockées dans un seul compartiment de table AWS géré. Ces compartiments de tables AWS gérés sont nommés `aws-s3` et ont le format Amazon Resource Name (ARN) suivant :

`arn:aws:s3tables:`*`region`*`:`*`account_id`*`:bucket/aws-s3`

Par exemple, si votre identifiant de compte est 123456789012 et que votre compartiment à usage général se trouve dans l'est des États-Unis (Virginie du Nord) (`us-east-1`), votre compartiment de table AWS géré est également créé dans l'est des États-Unis (Virginie du Nord) (`us-east-1`) et possède l'ARN suivant :

`arn:aws:s3tables:`*`us-east-1`*`:123456789012:bucket/aws-s3`

Par défaut, les compartiments de tables AWS gérés sont chiffrés par chiffrement côté serveur à l'aide de clés gérées Amazon S3 (SSE-S3). Après avoir créé votre première configuration de métadonnées, vous pouvez définir le paramètre de chiffrement par défaut pour le compartiment de table AWS géré afin d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Pour plus d'informations, consultez les sections Chiffrement pour les compartiments de tables AWS gérés etthe section called "Spécification de SSE-KMS".

Dans votre compartiment de tables AWS géré, les tables de métadonnées de votre configuration sont généralement stockées dans un espace de noms au format de dénomination suivant :

b_*`general-purpose-bucket-name`*

Pour plus d'informations sur les espaces de noms des tables de métadonnées, consultezthe section called "Fonctionnement des tables de métadonnées".

Lorsque vous créez la configuration de votre table de métadonnées, vous pouvez choisir de chiffrer vos tables de métadonnées AWS gérées avec un chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Si vous choisissez d'utiliser SSE-KMS, vous devez fournir une clé KMS gérée par le client dans la même région que votre bucket à usage général. Vous pouvez définir le type de chiffrement de vos tables uniquement lors de leur création. Une fois qu'une table AWS gérée est créée, vous ne pouvez pas modifier ses paramètres de chiffrement. Pour spécifier SSE-KMS pour vos tables de métadonnées, vous devez disposer de certaines autorisations. Pour plus d'informations, consultez la section Autorisations pour SSE-KMS.

Le paramètre de chiffrement d'une table de métadonnées a priorité sur le paramètre de chiffrement par défaut au niveau du compartiment. Si vous ne spécifiez pas de chiffrement pour une table, celle-ci héritera du paramètre de chiffrement par défaut du compartiment.

AWS les compartiments de tables gérés ne sont pas pris en compte dans vos quotas de tables S3. Pour plus d'informations sur l'utilisation des compartiments de tables AWS gérés et des tables AWS gérées, consultez la section Utilisation des compartiments de tables AWS gérés.

Vous pouvez créer une configuration de table de métadonnées à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

> **Note**
>
> - Si vous avez créé votre configuration de métadonnées S3 avant le 15 juillet 2025, nous vous recommandons de la supprimer et de la recréer afin de pouvoir faire expirer les enregistrements des tables de journal et créer une table d'inventaire. Pour de plus amples informations, veuillez consulter the section called "Activation des tables d'inventaire sur les configurations de métadonnées créées avant le 15 juillet 2025".
> - Si vous avez supprimé la configuration de votre table de métadonnées et que vous souhaitez recréer une configuration pour le même compartiment à usage général, vous devez d'abord supprimer manuellement les anciennes tables de journal et d'inventaire de votre compartiment de tables AWS géré. Dans le cas contraire, la création de la nouvelle configuration de table de métadonnées échoue car ces tables existent déjà. Pour supprimer vos tables de métadonnées, consultezthe section called "Suppression d'une table de métadonnées".
>
> La suppression d'une configuration de table de métadonnées entraîne uniquement la suppression de la configuration. Le bucket de table AWS géré et vos tables de métadonnées existent toujours, même si vous supprimez la configuration des tables de métadonnées.

Prérequis

Avant de créer une configuration de table de métadonnées, assurez-vous de remplir les conditions préalables suivantes :

- Avant de créer une configuration de table de métadonnées, assurez-vous que vous disposez des autorisations AWS Identity and Access Management (IAM) nécessaires pour créer et gérer des tables de métadonnées. Pour de plus amples informations, veuillez consulter the section called "Autorisations pour les tables de métadonnées".

- Si vous envisagez d'interroger vos tables de métadonnées avec Amazon Athena ou un autre moteur de AWS requête, assurez-vous d'intégrer votre compartiment de tables AWS géré aux services AWS d'analyse. Pour de plus amples informations, veuillez consulter the section called "Utilisation de tables S3 avec des services AWS d'analyse".

  Si vous avez déjà intégré un bucket de table existant dans cette région, votre bucket de table AWS géré est également intégré automatiquement. Pour déterminer le statut d'intégration de vos compartiments de table dans cette région, ouvrez la console Amazon S3 et choisissez Buckets de table dans le volet de navigation de gauche. Sous Intégration aux services AWS d'analyse, vérifiez la région et vérifiez si le statut d'intégration indique Activé.

Création de la configuration d'une table de métadonnées

Utilisation de la console S3

Pour créer la configuration d'une table de métadonnées

Avant de créer la configuration d'une table de métadonnées, assurez-vous que vous avez vérifié les prérequis, que vous les respectez et que vous avez passé en revue the section called "Limites et restrictions".

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Choisissez le compartiment à usage général pour lequel vous souhaitez créer une configuration de table de métadonnées.

   > **Note**
   >
   > Assurez-vous que ce seau à usage général est un Région AWS endroit où des seaux de table sont disponibles. Les compartiments de tables ne sont disponibles que dans les régions USA Est (Virginie du Nord), USA Est (Ohio) et USA Ouest (Oregon).

4. Sur la page de détails du bucket, choisissez l'onglet Metadata.
5. Dans l'onglet Métadonnées, choisissez Créer une configuration de métadonnées.
6. Sur la page de configuration des métadonnées de création, sous Table du journal, vous pouvez choisir de chiffrer votre table avec un chiffrement côté serveur à l'aide de clés AWS Key

Management Service (AWS KMS) (SSE-KMS). Par défaut, les tables de journal sont chiffrées par chiffrement côté serveur à l'aide de clés gérées par Amazon S3 (SSE-S3).

Si vous choisissez d'utiliser SSE-KMS, vous devez fournir une clé KMS gérée par le client dans la même région que votre bucket à usage général.

> **Important**
>
> Vous pouvez définir le type de chiffrement pour vos tables de métadonnées uniquement lors de leur création. Une fois qu'une table AWS gérée est créée, vous ne pouvez pas modifier ses paramètres de chiffrement.

- Pour chiffrer votre table de journal avec SSE-S3 (valeur par défaut), choisissez Ne pas spécifier le type de cryptage.
- Pour chiffrer votre table de journal avec SSE-KMS, choisissez Spécifier le type de cryptage. Sous Type de chiffrement, choisissez Chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Sous AWS KMS clé, choisissez parmi vos clés KMS existantes ou entrez l'ARN de votre clé KMS. Si vous ne possédez pas encore de clé KMS, choisissez Enter KMS key ARN, puis Create a KMS key.

  Assurez-vous d'avoir configuré les autorisations nécessaires pour SSE-KMS. Pour plus d'informations, consultez la section Autorisations pour SSE-KMS.

7. (Facultatif) Par défaut, les enregistrements de votre table de journal n'expirent pas. Pour minimiser les coûts de stockage de votre table de journal, choisissez Activé pour l'expiration des enregistrements.

   Si vous activez l'expiration des enregistrements de table de journal, vous pouvez définir le nombre de jours pendant lesquels vos enregistrements de table de journal seront conservés. Pour définir la valeur des jours après lesquels les enregistrements expirent, vous pouvez spécifier n'importe quel nombre entier compris entre 7 et`2147483647`. Par exemple, pour conserver les enregistrements de votre table de journal pendant un an, définissez cette valeur sur`365`.

   Les dossiers expireront dans les 24 à 48 heures suivant leur éligibilité à l'expiration.

> **Important**
>
> Une fois que les enregistrements des tables de journal ont expiré, ils ne peuvent pas être récupérés.

Dans le tableau du journal, les enregistrements expireront après le nombre de jours spécifié, cochez la case.

8. (Facultatif) Si vous souhaitez ajouter une table d'inventaire à la configuration de votre table de métadonnées, sous Table d'inventaire dynamique, choisissez Activé pour le statut de configuration.

   Vous pouvez choisir de chiffrer votre table avec un chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Par défaut, les tables d'inventaire sont chiffrées par chiffrement côté serveur à l'aide de clés gérées par Amazon S3 (SSE-S3).

   Si vous choisissez d'utiliser SSE-KMS, vous devez fournir une clé KMS gérée par le client dans la même région que votre bucket à usage général.

   > **Important**
   >
   > Vous pouvez définir le type de chiffrement pour vos tables de métadonnées uniquement lors de leur création. Une fois qu'une table AWS gérée est créée, vous ne pouvez pas modifier ses paramètres de chiffrement.

   - Pour chiffrer votre table d'inventaire avec SSE-S3 (valeur par défaut), choisissez Ne pas spécifier le type de cryptage.
   - Pour chiffrer votre table d'inventaire avec SSE-KMS, choisissez Spécifier le type de cryptage. Sous Type de chiffrement, choisissez Chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Sous AWS KMS clé, choisissez parmi vos clés KMS existantes ou entrez l'ARN de votre clé KMS. Si vous ne possédez pas encore de clé KMS, choisissez Enter KMS key ARN, puis Create a KMS key.

     Assurez-vous d'avoir configuré les autorisations nécessaires pour SSE-KMS. Pour plus d'informations, consultez la section Autorisations pour SSE-KMS.

9. Choisissez Créer une configuration de table de métadonnées.

Si la configuration de votre table de métadonnées est réussie, les noms et ceux ARNs de vos tables de métadonnées sont affichés dans l'onglet Métadonnées, ainsi que le nom du compartiment et de l'espace de noms de votre compartiment de table AWS géré.

Si vous avez choisi d'activer une table d'inventaire pour la configuration de votre table de métadonnées, la table est soumise à un processus appelé backfilling, au cours duquel Amazon S3 analyse votre compartiment à usage général pour récupérer les métadonnées initiales de tous les objets présents dans le compartiment. Selon le nombre d'objets contenus dans votre compartiment, ce processus peut prendre de quelques minutes (minimum 15 minutes) à plusieurs heures. Lorsque le processus de remblayage est terminé, le statut de votre tableau d'inventaire passe de Remblayage à Actif. Une fois le remblayage terminé, les mises à jour apportées à vos objets sont généralement reflétées dans le tableau d'inventaire en moins d'une heure.

Pour surveiller les mises à jour apportées à la configuration de votre table de métadonnées, vous pouvez utiliser AWS CloudTrail. Pour de plus amples informations, veuillez consulter the section called “Actions au niveau du compartiment Amazon S3 suivies par journalisation CloudTrail ”.

À l'aide du AWS CLI

Pour exécuter les commandes suivantes, vous devez les avoir AWS CLI installées et configurées. Si ce n'est pas le cas AWS CLI , consultez la section Installer ou mettre à jour vers la dernière version du AWS CLI Guide de l'AWS Command Line Interface utilisateur.

Vous pouvez également exécuter des AWS CLI commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? et Mise en route AWS CloudShell dans le guide de AWS CloudShell l'utilisateur.

Pour créer une configuration de table de métadonnées à l'aide du AWS CLI

Avant de créer la configuration d’une table de métadonnées, assurez-vous que vous avez vérifié les prérequis, que vous les respectez et que vous avez passé en revue the section called “Limites et restrictions”.

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

1. Créez un fichier JSON contenant la configuration de votre table de métadonnées et enregistrez-le (par exemple, `metadata-config.json`). Voici un exemple de configuration.

Vous devez indiquer si vous souhaitez activer ou désactiver l'expiration des enregistrements de la table de journal. Si vous choisissez d'activer l'expiration des enregistrements, vous devez également spécifier le nombre de jours après lesquels les enregistrements de votre table de journal expireront. Pour définir la `Days` valeur, vous pouvez spécifier n'importe quel nombre entier compris entre 7 et`2147483647`. Par exemple, pour conserver les enregistrements de votre table de journal pendant un an, définissez cette valeur sur`365`.

Vous pouvez éventuellement choisir de configurer une table d'inventaire.

Pour les tables de journal et les tables d'inventaire, vous pouvez éventuellement spécifier une configuration de chiffrement. Par défaut, les tables de métadonnées sont chiffrées par chiffrement côté serveur à l'aide de clés gérées Amazon S3 (SSE-S3), que vous pouvez spécifier en configurant sur. `SseAlgorithm` `AES256`

Pour chiffrer vos tables de métadonnées à l'aide d'un chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS), définissez sur. `SseAlgorithm` `aws:kms` Vous devez également utiliser l'ARN d'une clé KMS gérée par le client dans la même région que celle où se trouve votre bucket à usage général. `KmsKeyArn`

```
{
  "JournalTableConfiguration": {
     "RecordExpiration": {
       "Expiration": "ENABLED",
       "Days": 10
    },
    "EncryptionConfiguration": {
      "SseAlgorithm": "AES256"
    }
  },
  "InventoryTableConfiguration": {
    "ConfigurationState": "ENABLED",
    "EncryptionConfiguration": {
      "SseAlgorithm": "aws:kms",
      "KmsKeyArn": "arn:aws:kms:us-east-2:account-id:key/key-id"
    }
  }
}
```

2. Utilisez la commande suivante pour appliquer la configuration de la table de métadonnées à votre compartiment à usage général (par exemple, *`amzn-s3-demo-bucket`*) :

```
aws s3api create-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--metadata-configuration file://./metadata-config.json \
--region us-east-2
```

3. Pour vérifier si la configuration a été créée, utilisez la commande suivante :

```
aws s3api get-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--region us-east-2
```

Pour surveiller les mises à jour apportées à la configuration de votre table de métadonnées, vous pouvez utiliser AWS CloudTrail. Pour de plus amples informations, veuillez consulter the section called “Actions au niveau du compartiment Amazon S3 suivies par journalisation CloudTrail ”.

Utilisation de l'API REST

Vous pouvez envoyer des demandes REST pour créer la configuration d'une table de métadonnées. Pour plus d'informations, consultez CreateBucketMetadataConfiguration dans la Référence d'API Amazon S3.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour créer une configuration de table de métadonnées dans Amazon S3. Pour plus d'informations, consultez la liste des applications prises SDKs en charge dans le manuel Amazon S3 API Reference.

Activation des tables d'inventaire sur les configurations de métadonnées créées avant le 15 juillet 2025

Si vous avez créé votre configuration de métadonnées S3 avant le 15 juillet 2025, nous vous recommandons de la supprimer et de la recréer afin de pouvoir faire expirer les enregistrements des tables de journal et créer une table d'inventaire. Les modifications apportées à votre bucket à usage général entre la suppression de l'ancienne configuration et la création de la nouvelle ne sont enregistrées dans aucune de vos tables de journal.

Pour migrer d'une ancienne configuration de métadonnées vers une nouvelle configuration, procédez comme suit :

1. Supprimez la configuration de votre table de métadonnées existante. Pour step-by-step obtenir des instructions, voirthe section called "Suppression de configurations de tables de métadonnées".
2. Créez une nouvelle configuration de table de métadonnées. Pour step-by-step obtenir des instructions, voirthe section called "Création de tables de métadonnées".

Si vous avez besoin d'aide pour migrer votre configuration, contactez AWS Support.

Après avoir créé votre nouvelle configuration de métadonnées, vous disposerez de deux tables de journal. Si vous n'avez plus besoin de l'ancienne table de journal, vous pouvez la supprimer. Pour step-by-step obtenir des instructions, voirthe section called "Suppression des tables de métadonnées". Si vous avez conservé votre ancienne table de journal et que vous souhaitez la joindre à la nouvelle, consultez the section called "Jonction de métadonnées personnalisées" des exemples illustrant comment joindre deux tables.

Après la migration, vous pouvez effectuer les opérations suivantes :

1. Pour consulter votre configuration, vous pouvez désormais utiliser l'opération `GetBucketMetadataConfiguration` API. Pour déterminer si votre configuration est ancienne ou nouvelle, vous pouvez consulter l'attribut suivant de votre réponse d'`GetBucketMetadataConfiguration`API. Un type de compartiment AWS géré (`"aws"`) indique une nouvelle configuration, et un type de compartiment géré par le client (`"customer"`) indique une ancienne configuration.

   ```
   "MetadataTableConfigurationResult": {
              "TableBucketType": ["aws" | "customer"]
   ```

   Pour de plus amples informations, veuillez consulter the section called "Afficher les configurations des tables de métadonnées".

   > **Note**
   >
   > Vous pouvez utiliser les opérations `GetBucketMetadataConfiguration` et `DeleteBucketMetadataConfiguration` API avec les anciennes ou les nouvelles configurations de tables de métadonnées. Toutefois, si vous essayez d'utiliser les opérations `GetBucketMetadataTableConfiguration` et `DeleteBucketMetadataTableConfiguration` API avec de nouvelles configurations, vous recevrez des `405 Method Not Allowed` erreurs HTTP.

Assurez-vous de mettre à jour vos processus afin d'utiliser les nouvelles opérations d'API (`CreateBucketMetadataConfigurationGetBucketMetadataConfiguration`, `etDeleteBucketMetadataConfiguration`) au lieu des anciennes opérations d'API.

2. Si vous envisagez d'interroger vos tables de métadonnées avec Amazon Athena ou un autre moteur de AWS requête, assurez-vous d'intégrer votre compartiment de tables AWS géré aux services AWS d'analyse. Si vous avez déjà intégré un bucket de table existant dans cette région, votre bucket de table AWS géré est également intégré automatiquement. Pour de plus amples informations, veuillez consulter the section called “Utilisation de tables S3 avec des services AWS d'analyse”.

Contrôle de l'accès aux tables de métadonnées

Pour contrôler l'accès à vos tables de métadonnées Amazon S3, vous pouvez utiliser des politiques basées sur les ressources AWS Identity and Access Management (IAM) associées à votre compartiment de tables et à vos tables de métadonnées. En d'autres termes, vous pouvez contrôler l'accès à vos tables de métadonnées à la fois au niveau du compartiment de tables et au niveau de la table.

Pour plus d'informations sur le contrôle de l'accès à vos compartiments de tables et à vos tables, consultez Gestion des accès pour les tables S3.

Important

Lorsque vous créez ou mettez à jour des politiques de compartiment ou de table, assurez-vous de ne pas restreindre les principes du service Amazon S3 `metadata.s3.amazonaws.com` et `maintenance.s3tables.amazonaws.com` de ne pas écrire dans votre compartiment de table ou dans vos tables de métadonnées.
Si Amazon S3 ne parvient pas à écrire dans votre compartiment de tables ou dans vos tables de métadonnées, vous devez supprimer votre configuration de métadonnées, supprimer vos tables de métadonnées, puis créer une nouvelle configuration. Si votre configuration comportait une table d'inventaire, une nouvelle table d'inventaire doit être créée, et le remplissage de la nouvelle table d'inventaire vous sera facturé à nouveau.

Vous pouvez également contrôler l'accès aux lignes et aux colonnes de vos tables de métadonnées via AWS Lake Formation. Pour plus d'informations, consultez Gestion des autorisations Lake

Formation et Filtrage des données et sécurité au niveau des cellules dans Lake Formation dans le Guide du développeur AWS Lake Formation .

Enregistrements de table de journal expirant

Par défaut, les enregistrements de votre table de journal n'expirent pas. Pour minimiser les coûts de stockage de votre table de journal, vous pouvez activer l'expiration des enregistrements de la table de journal.

> **Note**
>
> Si vous avez créé votre configuration de métadonnées S3 avant le 15 juillet 2025, vous ne pouvez pas activer l'expiration des enregistrements de la table de journal sur cette configuration. Nous vous recommandons de supprimer et de recréer votre configuration afin de pouvoir faire expirer les enregistrements des tables de journal et créer une table d'inventaire. Pour de plus amples informations, veuillez consulter the section called "Activation des tables d'inventaire sur les configurations de métadonnées créées avant le 15 juillet 2025".

Si vous activez l'expiration des enregistrements de table de journal, vous pouvez définir le nombre de jours pendant lesquels vos enregistrements de table de journal seront conservés. Pour définir cette valeur, spécifiez un nombre entier compris entre 7 et2147483647. Par exemple, pour conserver les enregistrements de votre table de journal pendant un an, définissez cette valeur sur365.

> **Important**
>
> Une fois que les enregistrements des tables de journal ont expiré, ils ne peuvent pas être récupérés.

Les dossiers expirent dans les 24 à 48 heures suivant leur éligibilité à l'expiration. Les enregistrements du journal sont supprimés du dernier instantané. Les données et le stockage des enregistrements supprimés sont supprimés par le biais d'opérations de maintenance des tables.

Si vous avez activé l'expiration des enregistrements de table de journal, vous pouvez la désactiver à tout moment pour arrêter l'expiration de vos enregistrements de table de journal.

Vous pouvez faire expirer les enregistrements des tables de journal à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

Comment faire expirer les enregistrements d'une table de journal

Utilisation de la console S3

Pour faire expirer les enregistrements d'une table de journal

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Choisissez le compartiment à usage général qui contient la configuration de la table de métadonnées avec la table de journal dont vous souhaitez faire expirer les enregistrements.
4. Sur la page de détails du bucket, choisissez l'onglet Metadata.
5. Dans l'onglet Métadonnées, choisissez Modifier, puis Modifier l'expiration des enregistrements de la table des journaux.
6. Sur la page Modifier l'expiration des enregistrements de la table de journal, choisissez Activé sous Expiration des enregistrements.
7. Définissez le nombre de jours pendant lesquels vous souhaitez conserver les enregistrements de votre table de journal. Pour définir la valeur Jours après lesquels les enregistrements expirent, spécifiez un nombre entier compris entre 7 et2147483647. Par exemple, pour conserver les enregistrements de votre table de journal pendant un an, définissez cette valeur sur365.

   > **Important**
   >
   > Une fois que les enregistrements des tables de journal ont expiré, ils ne peuvent pas être récupérés.

8. Dans le tableau du journal, les enregistrements expireront après le nombre de jours spécifié, cochez la case.
9. Sélectionnez Enregistrer les modifications.

Si vous souhaitez désactiver l'expiration des enregistrements de la table de journal, répétez les étapes précédentes, mais choisissez Désactivé au lieu de Activé pour l'étape 6.

À l'aide du AWS CLI

Pour exécuter les commandes suivantes, vous devez les avoir AWS CLI installées et configurées. Si ce n'est pas le cas AWS CLI , consultez la section Installer ou mettre à jour vers la dernière version du AWS CLI Guide de l'AWS Command Line Interface utilisateur.

Vous pouvez également exécuter AWS CLI des commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? et Mise en route AWS CloudShell dans le guide de AWS CloudShell l'utilisateur.

Pour faire expirer les enregistrements d'une table de journal à l'aide du AWS CLI

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

1. Créez un fichier JSON contenant la configuration de votre table de journal et enregistrez-le (par exemple,`journal-config.json`). Voici un exemple de configuration.

   Pour définir la `Days` valeur, spécifiez un nombre entier compris entre 7 et`2147483647`. Par exemple, pour conserver les enregistrements de votre table de journal pendant un an, définissez cette valeur sur`365`.

   ```
   {
     "RecordExpiration": {
       "Expiration": "ENABLED",
       "Days": 10
     }
   }
   ```

   Pour désactiver l'expiration des enregistrements de la table de journal, créez plutôt l'exemple de configuration suivant. S'il `Expiration` est défini sur`DISABLED`, vous ne devez pas spécifier de `Days` valeur dans la configuration.

   ```
   {
     "RecordExpiration": {
       "Expiration": "DISABLED"
     }
   }
   ```

2. Utilisez la commande suivante pour faire expirer les enregistrements de la table de journal dans votre compartiment à usage général (par exemple,*amzn-s3-demo-bucket*) :

```
aws s3api update-bucket-metadata-journal-table-configuration \
--bucket amzn-s3-demo-bucket \
--journal-table-configuration file://./journal-config.json \
--region us-east-2
```

Utilisation de l'API REST

Vous pouvez envoyer des requêtes REST pour faire expirer les enregistrements d'une table de journal. Pour de plus amples informations, veuillez consulter UpdateBucketMetadataJournalTableConfiguration.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour faire expirer les enregistrements des tables de journal dans Amazon S3. Pour plus d'informations, consultez la liste des produits pris en charge SDKs.

Activation ou désactivation des tables d'inventaire dynamiques

Par défaut, la configuration de votre table de métadonnées contient une table de journal qui enregistre les événements qui se produisent pour les objets de votre compartiment. La table de journal est obligatoire pour chaque configuration de table de métadonnées.

Vous pouvez éventuellement ajouter une table d'inventaire dynamique à la configuration de votre table de métadonnées. Le tableau d'inventaire en temps réel fournit un inventaire simple et interrogeable de tous les objets et de leurs versions dans votre compartiment afin que vous puissiez déterminer l'état le plus récent de vos données.

> **Note**
>
> Si vous avez créé votre configuration de métadonnées S3 avant le 15 juillet 2025, vous ne pouvez pas activer de table d'inventaire sur cette configuration. Nous vous recommandons de supprimer et de recréer votre configuration afin de pouvoir créer une table d'inventaire et faire expirer les enregistrements des tables de journal. Pour de plus amples informations, veuillez consulter the section called “Activation des tables d'inventaire sur les configurations de métadonnées créées avant le 15 juillet 2025”.

Le tableau d'inventaire contient les dernières métadonnées pour tous les objets de votre compartiment. Vous pouvez utiliser ce tableau pour simplifier et accélérer les flux de travail métier et les tâches liées au Big Data en identifiant les objets que vous souhaitez traiter pour différentes charges de travail. Par exemple, vous pouvez interroger la table d'inventaire pour effectuer les opérations suivantes :

- Trouvez tous les objets stockés dans la classe de stockage S3 Glacier Deep Archive.
- Créez une distribution de balises d'objets ou recherchez des objets sans balises.
- Trouvez tous les objets qui ne sont pas chiffrés à l'aide du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS).
- Comparez votre tableau d'inventaire à deux moments différents pour comprendre l'augmentation du nombre d'objets dotés de balises spécifiques.

Si vous avez choisi d'activer une table d'inventaire pour la configuration de votre table de métadonnées, la table est soumise à un processus appelé backfilling, au cours duquel Amazon S3 analyse votre compartiment à usage général pour récupérer les métadonnées initiales de tous les objets présents dans le compartiment. Selon le nombre d'objets contenus dans votre compartiment, ce processus peut prendre de quelques minutes (minimum 15 minutes) à plusieurs heures. Lorsque le processus de remblayage est terminé, le statut de votre tableau d'inventaire passe de Remblayage à Actif. Une fois le remblayage terminé, les mises à jour apportées à vos objets sont généralement reflétées dans le tableau d'inventaire en moins d'une heure.

> **Note**
>
> - Le remplissage de votre tableau d'inventaire vous est facturé. Si votre bucket à usage général contient plus d'un milliard d'objets, des frais mensuels vous sont également facturés pour votre tableau d'inventaire. Pour plus d'informations, consultez Tarification Amazon S3.
> - Vous ne pouvez pas suspendre les mises à jour de votre tableau d'inventaire puis les reprendre. Vous pouvez toutefois désactiver la configuration de la table d'inventaire. La désactivation de la table d'inventaire ne la supprime pas. Le tableau d'inventaire est conservé pour vos dossiers jusqu'à ce que vous décidiez de le supprimer.
>
>   Si vous avez désactivé votre table d'inventaire et souhaitez la réactiver ultérieurement, vous devez d'abord supprimer l'ancienne table d'inventaire de votre compartiment de tables AWS géré. Lorsque vous réactivez la configuration de la table d'inventaire, Amazon S3

crée une nouvelle table d'inventaire et vous êtes à nouveau débité pour le remplissage de la nouvelle table d'inventaire.

Vous pouvez activer ou désactiver les tables d'inventaire à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

Prérequis

Si vous avez désactivé votre table d'inventaire et souhaitez maintenant la réactiver, vous devez d'abord supprimer manuellement l'ancienne table d'inventaire de votre compartiment de tables AWS géré. Dans le cas contraire, la réactivation de la table d'inventaire échoue car une table d'inventaire existe déjà dans le compartiment de tables. Pour supprimer votre tableau d'inventaire, consultezthe section called "Suppression d'une table de métadonnées".

Lorsque vous réactivez la configuration de la table d'inventaire, Amazon S3 crée une nouvelle table d'inventaire et vous êtes à nouveau débité pour le remplissage de la nouvelle table d'inventaire.

Activer ou désactiver les tables d'inventaire

Utilisation de la console S3

Pour activer ou désactiver les tables d'inventaire

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Choisissez le compartiment à usage général avec la configuration de table de métadonnées pour laquelle vous souhaitez activer ou désactiver une table d'inventaire.
4. Sur la page de détails du bucket, choisissez l'onglet Metadata.
5. Dans l'onglet Métadonnées, choisissez Modifier, puis Modifier la configuration de la table d'inventaire.
6. Sur la page de configuration Modifier la table d'inventaire, choisissez Activé ou Désactivé sous Table d'inventaire.

> **Note**
>
> Avant de choisir Activé, assurez-vous d'avoir vérifié et rempli les conditions requises.

- Si vous avez choisi Activé, vous pouvez choisir de chiffrer votre table à l'aide du chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Par défaut, les tables d'inventaire sont chiffrées par chiffrement côté serveur à l'aide de clés gérées par Amazon S3 (SSE-S3).

  Si vous choisissez d'utiliser SSE-KMS, vous devez fournir une clé KMS gérée par le client dans la même région que votre bucket à usage général.

  > **Important**
  >
  > Vous pouvez définir le type de chiffrement pour vos tables de métadonnées uniquement lors de leur création. Une fois qu'une table AWS gérée est créée, vous ne pouvez pas modifier ses paramètres de chiffrement.

  - Pour chiffrer votre table d'inventaire avec SSE-S3 (valeur par défaut), choisissez Ne pas spécifier le type de cryptage.
  - Pour chiffrer votre table d'inventaire avec SSE-KMS, choisissez Spécifier le type de cryptage. Sous Type de chiffrement, choisissez Chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Sous AWS KMS clé, choisissez parmi vos clés KMS existantes ou entrez l'ARN de votre clé KMS. Si vous ne possédez pas encore de clé KMS, choisissez Enter KMS key ARN, puis Create a KMS key.
- Si vous avez choisi Désactivé, sous Une fois la table d'inventaire désactivée, la table ne sera plus mise à jour et les mises à jour ne pourront pas être reprises, cochez la case.

7. Sélectionnez Enregistrer les modifications.

À l'aide du AWS CLI

Pour exécuter les commandes suivantes, vous devez les avoir AWS CLI installées et configurées. Si ce n'est pas le cas AWS CLI , consultez la section Installer ou mettre à jour vers la dernière version du AWS CLI Guide de l'AWS Command Line Interface utilisateur.

Vous pouvez également exécuter des AWS CLI commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? et Mise en route AWS CloudShell dans le guide de AWS CloudShell l'utilisateur.

Pour activer ou désactiver les tableaux d'inventaire à l'aide du AWS CLI

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

> **Note**
>
> Avant d'activer une configuration d'inventaire, assurez-vous d'avoir passé en revue et de respecter les conditions préalables.

1. Créez un fichier JSON contenant la configuration de votre table d'inventaire et enregistrez-le (par exemple,`inventory-config.json`). Voici un exemple de configuration permettant d'activer une nouvelle table d'inventaire.

   Si vous activez une table d'inventaire, vous pouvez éventuellement spécifier une configuration de chiffrement. Par défaut, les tables de métadonnées sont chiffrées par chiffrement côté serveur à l'aide de clés gérées Amazon S3 (SSE-S3), que vous pouvez spécifier en configurant sur. `SseAlgorithm` `AES256`

   Pour chiffrer votre table d'inventaire avec un chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS), définissez sur. `SseAlgorithm` `aws:kms` Vous devez également utiliser l'ARN d'une clé KMS gérée par le client dans la même région que celle où se trouve votre bucket à usage général. `KmsKeyArn`

   ```
   {
     "ConfigurationState": "ENABLED",
     "EncryptionConfiguration": {
       "SseAlgorithm": "aws:kms",
       "KmsKeyArn": "arn:aws:kms:us-east-2:account-id:key/key-id"
     }
   }
   ```

   Si vous souhaitez désactiver une table d'inventaire existante, utilisez la configuration suivante :

   ```
   {
     "ConfigurationState": "DISABLED"  }
   }
   ```

2. Utilisez la commande suivante pour mettre à jour la configuration de la table d'inventaire pour votre compartiment à usage général (par exemple,*amzn-s3-demo-bucket*) :

```
aws s3api update-bucket-metadata-inventory-table-configuration \
--bucket amzn-s3-demo-source-bucket \
--inventory-table-configuration file://./inventory-config.json \
--region us-east-2
```

Utilisation de l'API REST

Vous pouvez envoyer des requêtes REST pour activer ou désactiver les tables d'inventaire. Pour de plus amples informations, veuillez consulter UpdateBucketMetadataInventoryTableConfiguration.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour activer ou désactiver les tables d'inventaire dans Amazon S3. Pour plus d'informations, consultez la liste des produits pris en charge SDKs.

Afficher les configurations des tables de métadonnées

Si vous avez créé une configuration de table de métadonnées pour un bucket à usage général, vous pouvez consulter des informations sur la configuration, par exemple si une table d'inventaire a été activée ou si l'expiration des enregistrements de la table de journal a été activée. Vous pouvez également consulter l'état de votre journal et les tableaux d'inventaire.

Vous pouvez consulter la configuration de votre table de métadonnées pour un compartiment à usage général à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

Afficher la configuration d'une table de métadonnées

Utilisation de la console S3

Pour afficher la configuration d'une table de métadonnées

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Choisissez le compartiment à usage général qui contient la configuration de la table de métadonnées que vous souhaitez consulter.

4. Sur la page de détails du bucket, choisissez l'onglet Metadata.
5. Dans l'onglet Métadonnées, faites défiler l'écran jusqu'à la section Configuration des métadonnées. Dans les sections Table du journal et Table d'inventaire, vous pouvez consulter diverses informations relatives à ces configurations, telles que leurs noms de ressources Amazon (ARNs), le statut de vos tables et si vous avez activé l'expiration des enregistrements des tables de journal ou si vous avez activé l'expiration des enregistrements des tables de journal ou une table d'inventaire.

À l'aide du AWS CLI

Pour exécuter les commandes suivantes, vous devez les avoir AWS CLI installées et configurées. Si ce n'est pas le cas AWS CLI , consultez la section Installer ou mettre à jour vers la dernière version du AWS CLI Guide de l'AWS Command Line Interface utilisateur.

Vous pouvez également exécuter des AWS CLI commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? et Mise en route AWS CloudShell dans le guide de AWS CloudShell l'utilisateur.

Pour afficher la configuration d'une table de métadonnées à l'aide du AWS CLI

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

1. Utilisez la commande suivante pour afficher la configuration de la table de métadonnées de votre bucket à usage général (par exemple,*amzn-s3-demo-bucket*) :

```
aws s3api get-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--region us-east-2
```

2. Consultez le résultat de cette commande pour connaître l'état de la configuration de votre table de métadonnées. Par exemple :

```
{
    "GetBucketMetadataConfigurationResult": {
        "MetadataConfigurationResult": {
            "DestinationResult": {
                "TableBucketType": "aws",
```

```
                "TableBucketArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/
aws-managed-s3-111122223333-us-east-2",
                "TableNamespace": "b_general-purpose-bucket-name"
            },
            "JournalTableConfigurationResult": {
                "TableStatus": "ACTIVE",
                "TableName": "journal",
                "TableArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/aws-
managed-s3-111122223333-us-east-2/table/0f01234c-fe7a-492f-a4c7-adec3864ea85",
                "EncryptionConfiguration": {
                    "SseAlgorithm": "AES256"
                },
                "RecordExpiration": {
                    "Expiration": "ENABLED",
                    "Days": 10
                }
            },
            "InventoryTableConfigurationResult": {
                "ConfigurationState": "ENABLED",
                "TableStatus": "BACKFILL_COMPLETE",
                "TableName": "inventory",
                "TableArn": "arn:aws:s3tables:us-east-2:111122223333:bucket/aws-
managed-s3-111122223333-us-east-2/table/e123456-b876-4e5e-af29-bb055922ee4d",
                "EncryptionConfiguration": {
                    "SseAlgorithm": "AES256"
                }
            }
        }
    }
}
```

Utilisation de l'API REST

Vous pouvez envoyer des requêtes REST pour consulter la configuration d'une table de métadonnées. Pour de plus amples informations, veuillez consulter GetBucketMetadataTableConfiguration.

> **Note**
>
> Vous pouvez utiliser le fonctionnement de l'`GetBucketMetadataConfiguration`API V2 avec les configurations de tables de métadonnées V1 ou V2. Toutefois, si vous essayez

d'utiliser le fonctionnement de l'`GetBucketMetadataTableConfiguration`API V1 avec des configurations V2, vous recevrez une `405 Method Not Allowed` erreur HTTP.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour consulter la configuration d'une table de métadonnées dans Amazon S3. Pour plus d'informations, consultez la liste des produits pris en charge SDKs.

Suppression de configurations de tables de métadonnées

Si vous souhaitez arrêter de mettre à jour la configuration d'une table de métadonnées pour un compartiment à usage général Amazon S3, vous pouvez supprimer la configuration de la table de métadonnées attachée à votre compartiment. La suppression d'une configuration de table de métadonnées entraîne uniquement la suppression de la configuration. Le bucket de table AWS géré et vos tables de métadonnées existent toujours, même si vous supprimez la configuration des tables de métadonnées. Toutefois, les tables de métadonnées ne seront plus mises à jour.

> **Note**
>
> Si vous supprimez la configuration de votre table de métadonnées et souhaitez recréer une configuration pour le même compartiment à usage général, vous devez d'abord supprimer manuellement les anciennes tables de journal et d'inventaire de votre compartiment de tables AWS géré. Dans le cas contraire, la création de la nouvelle configuration de table de métadonnées échoue car ces tables existent déjà. Pour supprimer vos tables de métadonnées, consultezthe section called “Suppression des tables de métadonnées”.

Pour supprimer vos tables de métadonnées, consultezthe section called “Suppression d'une table de métadonnées”. Pour supprimer votre compartiment de tables, consultez Suppression de compartiments de table et DeleteTableBucket dans la Référence d'API Amazon S3.

Vous pouvez supprimer la configuration d'une table de métadonnées à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

Suppression de la configuration d'une table de métadonnées

Utilisation de la console S3

Pour supprimer la configuration d'une table de métadonnées

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Choisissez le compartiment à usage général à partir duquel vous souhaitez supprimer une configuration de table de métadonnées.
4. Sur la page de détails du bucket, choisissez l'onglet Metadata.
5. Dans l'onglet Métadonnées, choisissez Supprimer.
6. Dans la boîte de dialogue Supprimer la configuration des métadonnées, entrez **`confirm`** pour confirmer que vous souhaitez supprimer la configuration. Ensuite, choisissez Supprimer.

À l'aide du AWS CLI

Pour exécuter les commandes suivantes, vous devez les avoir AWS CLI installées et configurées. Si ce n'est pas le cas AWS CLI , consultez la section Installer ou mettre à jour vers la dernière version du AWS CLI Guide de l'AWS Command Line Interface utilisateur.

Vous pouvez également exécuter des AWS CLI commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? et Mise en route AWS CloudShell dans le guide de AWS CloudShell l'utilisateur.

Pour supprimer la configuration d'une table de métadonnées à l'aide du AWS CLI

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

1. Utilisez la commande suivante pour supprimer la configuration de la table de métadonnées de votre compartiment à usage général (par exemple, *`amzn-s3-demo-bucket`*) :

```
aws s3api delete-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--region us-east-2
```

2. Pour vérifier si la configuration a été supprimée, utilisez la commande suivante :

```
aws s3api get-bucket-metadata-configuration \
--bucket amzn-s3-demo-bucket \
--region us-east-2
```

Utilisation de l'API REST

Vous pouvez envoyer des demandes REST pour supprimer la configuration d'une table de métadonnées. Pour de plus amples informations, veuillez consulter DeleteBucketMetadataConfiguration.

> **Note**
>
> Vous pouvez utiliser le fonctionnement de l'`DeleteBucketMetadataConfiguration`API V2 avec les configurations de tables de métadonnées V1 ou V2. Toutefois, si vous essayez d'utiliser le fonctionnement de l'`DeleteBucketMetadataTableConfiguration`API V1 avec des configurations V2, vous recevrez une `405 Method Not Allowed` erreur HTTP.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour supprimer une configuration de table de métadonnées dans Amazon S3. Pour plus d'informations, consultez la liste des produits pris en charge SDKs.

Suppression des tables de métadonnées

Si vous souhaitez supprimer les tables de métadonnées que vous avez créées pour un compartiment à usage général Amazon S3, vous pouvez supprimer les tables de métadonnées de votre compartiment de tables AWS géré.

> **Note**
>
> Avant de supprimer une table de métadonnées, nous vous recommandons de supprimer d'abord la configuration de table de métadonnées associée dans votre bucket à usage général. Pour de plus amples informations, veuillez consulter the section called "Suppression de configurations de tables de métadonnées".

Pour supprimer votre compartiment de table AWS géré, consultez Supprimer des compartiments de table et DeleteTableBucketdans le manuel de référence des API Amazon S3. Avant de supprimer votre compartiment de table AWS géré, nous vous recommandons de supprimer toutes les configurations de table de métadonnées associées à ce compartiment. Vous devez également d'abord supprimer toutes les tables de métadonnées du compartiment.

Vous pouvez supprimer une table de métadonnées à l'aide de AWS Command Line Interface (AWS CLI) AWS SDKs, de ou de l'API REST Amazon S3.

Suppression d'une table de métadonnées

À l'aide du AWS CLI

Pour exécuter les commandes suivantes, vous devez les avoir AWS CLI installées et configurées. Si ce n'est pas le cas AWS CLI , consultez la section Installer ou mettre à jour vers la dernière version du AWS CLI Guide de l'AWS Command Line Interface utilisateur.

Vous pouvez également exécuter des AWS CLI commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? et Mise en route AWS CloudShell dans le guide de AWS CloudShell l'utilisateur.

Pour supprimer la configuration d'une table de métadonnées à l'aide du AWS CLI

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

1. Utilisez la commande suivante pour supprimer la table de métadonnées de votre bucket de table AWS géré :

```
aws s3tables delete-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/aws-s3 \
--namespace b_general-purpose-bucket-name \
--name journal \
--region us-east-2
```

2. Pour vérifier si la table a été supprimée, utilisez la commande suivante :

```
aws s3tables get-table \
--table-bucket-arn arn:aws:s3tables:us-east-2:111122223333:bucket/aws-s3 \
--namespace b_general-purpose-bucket-name \
```

```
--name journal \
--region us-east-2
```

Utilisation de l'API REST

Vous pouvez envoyer des demandes REST pour supprimer la configuration d'une table de métadonnées. Pour plus d'informations, consultez DeleteTable dans la Référence d'API Amazon S3.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour supprimer une configuration de table de métadonnées dans Amazon S3. Pour plus d'informations, consultez la liste des applications prises SDKs en charge dans le manuel Amazon S3 API Reference.

Interrogation des tables de métadonnées

Vos tables de métadonnées Amazon S3 sont stockées dans un compartiment de tables S3 AWS géré, qui fournit un stockage optimisé pour les données tabulaires. Pour interroger vos métadonnées, vous pouvez intégrer votre bucket de table à Amazon SageMaker Lakehouse. Cette intégration, qui utilise le AWS Glue Data Catalog et AWS Lake Formation, permet aux services AWS d'analyse de découvrir et d'accéder automatiquement aux données de votre table.

Une fois votre compartiment de tables intégré au AWS Glue Data Catalog, vous pouvez directement interroger vos tables de métadonnées à l'aide de services AWS d'analyse tels qu'Amazon Athena, Amazon EMR et Amazon Redshift. Vous pouvez également créer des tableaux de bord interactifs avec les données de vos requêtes à l'aide d'Amazon QuickSight.

Pour plus d'informations sur l'intégration de votre compartiment de table S3 AWS géré à Amazon SageMaker Lakehouse, consultez. the section called "Utilisation de tables S3 avec des services AWS d'analyse"

Vous pouvez également interroger vos tables de métadonnées avec Apache SparkApache Trino, et toute autre application prenant en charge le Apache Iceberg format en utilisant le point de terminaison AWS Glue Iceberg REST, le point de terminaison Iceberg REST Amazon S3 Tables ou le catalogue de tables Amazon S3 pour le catalogue Apache Iceberg client. Pour plus d'informations sur l'accès à vos tables de métadonnées, consultezthe section called "Accès aux tables".

Vous pouvez analyser vos tables de métadonnées à l'aide de n'importe quel moteur de requête compatible avec ce Apache Iceberg format. Par exemple, vous pouvez interroger vos tables de métadonnées pour effectuer les opérations suivantes :

- Découvrir les modèles et les tendances d'utilisation du stockage
- Auditez AWS Key Management Service (AWS KMS) l'utilisation des clés de chiffrement sur vos objets
- Rechercher des objets à l'aide de métadonnées définies par l'utilisateur et de balises d'objet
- Comprendre l'évolution des métadonnées d'objet au fil du temps
- Découvrez quand les objets sont mis à jour ou supprimés, y compris l' Compte AWS ID ou l'adresse IP à l'origine de la demande

Vous pouvez également joindre des tables de métadonnées gérées par S3 et des tables de métadonnées personnalisées, ce qui vous permet d'effectuer des requêtes sur plusieurs ensembles de données.

Considérations sur la tarification des requêtes

Une tarification supplémentaire s'applique à l'exécution de requêtes sur vos tables de métadonnées. Pour plus d'informations, consultez les informations tarifaires du moteur de requête que vous utilisez.

Pour plus d'informations sur la manière de mieux rentabiliser vos requêtes, consultez Optimisation des performances des requêtes des tables de métadonnées.

Rubriques

- Autorisations pour interroger les tables de métadonnées
- Interrogation de tables de métadonnées à l'aide de services AWS d'analyse
- Interrogation des tables de métadonnées à l'aide de moteurs de requêtes open source
- Optimisation des performances des requêtes des tables de métadonnées
- Exemples de requêtes de tables de métadonnées

Autorisations pour interroger les tables de métadonnées

Avant de pouvoir interroger votre journal de métadonnées S3 et vos tables d'inventaire en temps réel, vous devez disposer de certaines autorisations relatives aux tables S3. Si vos tables de métadonnées ont été chiffrées côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS), vous devez également être `kms:Decrypt` autorisé à déchiffrer les données de la table.

Lorsque vous créez la configuration de vos tables de métadonnées, celles-ci sont stockées dans un bucket de tables AWS géré. Toutes les configurations de tables de métadonnées de votre compte et de la même région sont stockées dans un seul compartiment de table AWS géré nomméaws-s3.

Pour interroger les tables de métadonnées, vous pouvez utiliser l'exemple de politique suivant. Pour utiliser cette politique, remplacez *user input placeholders* par vos propres informations.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"PermissionsToQueryMetadataTables",
         "Effect":"Allow",
         "Action":[
             "s3tables:GetTable",
             "s3tables:GetTableData",
             "s3tables:GetTableMetadataLocation",
             "kms:Decrypt"
         ],
         "Resource":[
            "arn:aws:s3tables:region:account_id:bucket/aws-s3",
            "arn:aws:s3tables:region:account_id:bucket/aws-s3/table/*"
         ]
       }
    ]
}
```

Interrogation de tables de métadonnées à l'aide de services AWS d'analyse

Vous pouvez interroger vos tables de métadonnées gérées par S3 à l'aide de services AWS d'analyse tels qu'Amazon Athena, Amazon Redshift et Amazon EMR.

Avant de pouvoir exécuter des requêtes, vous devez d'abord intégrer les compartiments de tables S3 AWS gérés dans votre région Compte AWS et dans les services d' AWS analyse.

Interrogation des tables de métadonnées avec Amazon Athena

Après avoir intégré vos compartiments de tables S3 AWS gérés aux services AWS d'analyse, vous pouvez commencer à interroger vos tables de métadonnées dans Athena. Dans vos requêtes, procédez comme suit :

- Spécifiez votre catalogue comme `s3tablescatalog/aws-s3` et votre base de données comme b_*general_purpose_bucket_name* (qui est généralement l'espace de noms de vos tables de métadonnées).

- Assurez-vous d'entourer les noms des espaces de noms de vos tables de métadonnées entre guillemets (") ou backticks (`), sinon la requête risque de ne pas fonctionner.

Pour plus d'informations, consultez Interrogation des tables Amazon S3 avec Athena.

Vous pouvez également exécuter des requêtes dans Athena depuis la console Amazon S3.

Utilisation de la console S3 et d'Amazon Athena

La procédure suivante utilise la console Amazon S3 pour accéder à l'éditeur de requêtes Athena afin que vous puissiez interroger une table avec Amazon Athena.

Pour interroger une table de métadonnées

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans l'onglet Compartiments à usage général, choisissez le compartiment contenant la configuration des métadonnées pour la table de métadonnées que vous souhaitez interroger.
4. Sur la page des détails du bucket, choisissez l'onglet Metadata.
5. Choisissez Table de requêtes avec Athena, puis choisissez l'un des exemples de requêtes pour les tables de journal ou d'inventaire.
6. La console Amazon Athena s'ouvre et l'éditeur de requêtes Athena apparaît avec un exemple de requête chargé pour vous. Modifiez cette requête en fonction de votre cas d'utilisation.

   Dans l'éditeur de requêtes, le champ Catalogue doit être renseigné avec s3tablescatalog/aws-s3. Le champ Base de données doit être renseigné avec l'espace de noms dans lequel votre table est stockée (par exemple, b_ ***general-purpose-bucket-name***).

   > **Note**
   >
   > Si vous ne voyez pas ces valeurs dans les champs Catalogue et Base de données, assurez-vous d'avoir intégré votre compartiment de tables AWS géré aux services AWS

d'analyse de cette région. Pour de plus amples informations, veuillez consulter the section called “Utilisation de tables S3 avec des services AWS d'analyse”.

7. Pour exécuter la requête, choisissez ensuite Run (Exécuter).

> **Note**
>
> - Si vous recevez le message d'erreur « Autorisations insuffisantes pour exécuter la requête. Le principal n'a aucun privilège sur la ressource spécifiée. » Lorsque vous essayez d'exécuter une requête dans Athena, vous devez obtenir les autorisations Lake Formation nécessaires sur la table. Pour de plus amples informations, veuillez consulter the section called “Octroi d'une autorisation sur une table ou une base de données”.
>
> Assurez-vous également que vous disposez des autorisations AWS Identity and Access Management (IAM) appropriées pour interroger les tables de métadonnées. Pour de plus amples informations, veuillez consulter the section called “Autorisations pour interroger les tables de métadonnées”.
> - Si le message d'erreur « Iceberg ne peut pas accéder à la ressource demandée » s'affiche lorsque vous essayez d'exécuter la requête, accédez à la AWS Lake Formation console et assurez-vous que vous vous êtes accordé des autorisations sur le catalogue de compartiments de tables et la base de données (espace de noms) que vous avez créés. Ne spécifiez pas de table lorsque vous accordez ces autorisations. Pour de plus amples informations, veuillez consulter the section called “Octroi d'une autorisation sur une table ou une base de données”.

Interrogation des tables de métadonnées avec Amazon Redshift

Après avoir intégré vos compartiments de tables S3 AWS gérés aux services AWS d'analyse, procédez comme suit :

- Créez un lien de ressource vers l'espace de noms de votre table de métadonnées (généralementb_*`general_purpose_bucket_name`*).
- Assurez-vous d'entourer les noms des espaces de noms de vos tables de métadonnées entre guillemets (") ou backticks (`), sinon la requête risque de ne pas fonctionner.

Une fois cela fait, vous pouvez commencer à interroger vos tables de métadonnées dans la console Amazon Redshift. Pour plus d'informations, consultez Accès aux tables Amazon S3 avec Amazon Redshift.

Interrogation des tables de métadonnées avec Amazon EMR

Pour interroger vos tables de métadonnées à l'aide d'Amazon EMR, vous devez créer un cluster Amazon EMR configuré pour vos tables de métadonnées Apache Iceberg et vous y connecter à l'aide de. Apache Spark Vous pouvez configurer cela en intégrant vos compartiments de tables S3 AWS gérés à des services d' AWS analyse ou en utilisant le catalogue de tables Amazon S3 open source pour le catalogue Iceberg client.

> **Note**
>
> Lorsque vous utilisez Apache Spark Amazon EMR ou d'autres moteurs tiers pour interroger vos tables de métadonnées, nous vous recommandons d'utiliser le point de terminaison Iceberg REST Amazon S3 Tables. Votre requête risque de ne pas s'exécuter correctement si vous n'utilisez pas ce point de terminaison. Pour de plus amples informations, veuillez consulter the section called "Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison".

Pour plus d'informations, consultez Accès aux tables Amazon S3 avec Amazon EMR.

Interrogation des tables de métadonnées à l'aide de moteurs de requêtes open source

Vous pouvez interroger vos tables de métadonnées gérées par S3 à l'aide de moteurs de requêtes open source, tels queApache Spark. Lorsque vous utilisez Apache Spark Amazon EMR ou d'autres moteurs tiers pour interroger vos tables de métadonnées, nous vous recommandons d'utiliser le point de terminaison Iceberg REST Amazon S3 Tables. Votre requête risque de ne pas s'exécuter correctement si vous n'utilisez pas ce point de terminaison. Pour de plus amples informations, veuillez consulter the section called "Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison".

Optimisation des performances des requêtes des tables de métadonnées

Les métadonnées S3 étant basées sur le format de Apache Iceberg table, vous pouvez optimiser les performances et le coût de vos requêtes de table de journal en utilisant des plages de temps spécifiques.

Par exemple, la requête SQL suivante indique le niveau de sensibilité des nouveaux objets d'un compartiment S3 à usage général :

```
SELECT key, object_tags['SensitivityLevel']
FROM "b_general-purpose-bucket-name"."journal"
WHERE record_type = 'CREATE'
GROUP BY object_tags['SensitivityLevel']
```

Cette requête analyse l'intégralité de la table du journal, ce qui peut prendre un certain temps à s'exécuter. Pour améliorer les performances, vous pouvez inclure la colonne `record_timestamp` pour vous concentrer sur une plage de temps spécifique. Nous vous recommandons également d'utiliser le nom de table complet, que vous pouvez trouver dans la console Amazon S3 sur la page de détails de configuration des métadonnées de l'onglet Métadonnées du compartiment à usage général. Voici une version mise à jour de la requête précédente qui examine les nouveaux objets du mois dernier :

```
SELECT key, object_tags['SensitivityLevel']
FROM b_general-purpose-bucket-name"."aws-s3.b_general-purpose-bucket-name.journal"
WHERE record_type = 'CREATE'
AND record_timestamp > (CURRENT_TIMESTAMP - interval '1' month)
GROUP BY object_tags['SensitivityLevel']
```

Pour améliorer les performances des requêtes sur les tables d'inventaire, assurez-vous de n'interroger que les colonnes minimales dont vous avez besoin.

Exemples de requêtes de tables de métadonnées

Les exemples suivants montrent comment obtenir différents types d'informations à partir de vos tables de métadonnées S3 à l'aide de requêtes SQL standard.

Gardez à l'esprit les points suivants lorsque vous utilisez ces exemples :

- Ces exemples sont conçus pour fonctionner avec Amazon Athena. Vous devrez peut-être les modifier pour qu'ils fonctionnent avec un autre moteur de requête.
- Assurez-vous de comprendre comment optimiser vos requêtes.
- b_*general-purpose-bucket-name*Remplacez-le par le nom de votre espace de noms.
- Pour obtenir la liste complète des colonnes prises en charge, consultez le Schéma des tables de journal des métadonnées S3 etthe section called "Schéma des tables d'inventaire en temps réel".

Table des matières

- Exemples de requêtes dans une table de journal
  - Recherche d'objets par extension de fichier
  - Affichage de la liste des suppressions d'objets
  - Répertorier les clés de AWS KMS chiffrement utilisées par vos objets
  - Affichage de la liste des objets qui n'utilisent pas de clés KMS
  - Liste des clés de AWS KMS chiffrement utilisées pour les PUT opérations au cours des 7 derniers jours
  - Liste des objets supprimés au cours des dernières 24 heures par S3 Lifecycle
  - Affichage de la liste des métadonnées fournies par Amazon Bedrock
  - Identification de l'état actuel de vos objets
- Exemples de requêtes de table d'inventaire
  - Découvrir les ensembles de données qui utilisent des balises spécifiques
  - Répertorier les objets non chiffrés avec SSE-KMS
  - Répertorier les objets générés par Amazon Bedrock
  - Génération de la dernière table d'inventaire
- Jonction de métadonnées personnalisées à des tables de métadonnées S3
- Visualisation des données des tables de métadonnées avec Amazon QuickSight

Exemples de requêtes dans une table de journal

Vous pouvez utiliser les exemples de requêtes suivants pour interroger les tables de votre journal.

Recherche d'objets par extension de fichier

La requête suivante renvoie des objets dotés d'une extension de fichier spécifique (`.jpg`dans ce cas) :

```
SELECT key FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal"
WHERE key LIKE '%.jpg'
AND record_type = 'CREATE'
```

Affichage de la liste des suppressions d'objets

La requête suivante renvoie les événements de suppression d'objets, y compris l' Compte AWS identifiant ou le principal AWS de service à l'origine de la demande :

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp, requester,
 source_ip_address, version_id
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal"
WHERE record_type = 'DELETE';
```

Répertorier les clés de AWS KMS chiffrement utilisées par vos objets

La requête suivante renvoie ARNs les clés AWS Key Management Service (AWS KMS) chiffrant vos objets :

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal";
```

Affichage de la liste des objets qui n'utilisent pas de clés KMS

La requête suivante renvoie des objets qui ne sont pas chiffrés à l'aide de AWS KMS clés :

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal"
WHERE encryption_status NOT IN ('SSE-KMS', 'DSSE-KMS')
AND record_type = 'CREATE';
```

Liste des clés de AWS KMS chiffrement utilisées pour les **PUT** opérations au cours des 7 derniers jours

La requête suivante renvoie ARNs les clés AWS Key Management Service (AWS KMS) chiffrant vos objets :

```
SELECT DISTINCT kms_key_arn
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal"
WHERE record_timestamp > (current_date - interval '7' day)
AND kms_key_arn is NOT NULL;
```

Liste des objets supprimés au cours des dernières 24 heures par S3 Lifecycle

La requête suivante renvoie la liste des objets expirés le dernier jour par S3 Lifecycle :

```
SELECT bucket, key, version_id, last_modified_date, record_timestamp, requester
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal"
WHERE requester = 's3.amazonaws.com'
AND record_type = 'DELETE'
AND record_timestamp > (current_date - interval '1' day)
```

Affichage de la liste des métadonnées fournies par Amazon Bedrock

Certains AWS services (comme Amazon Bedrock) chargent des objets sur Amazon S3. Vous pouvez interroger les métadonnées des objets fournies par ces services. Par exemple, la requête suivante inclut la `user_metadata` colonne permettant de déterminer si des objets ont été chargés par Amazon Bedrock dans un bucket à usage général :

```
SELECT DISTINCT bucket, key, sequence_number, record_type, record_timestamp,
 user_metadata
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal"
WHERE record_type = 'CREATE'
AND user_metadata['content-source'] = 'AmazonBedrock';
```

Si Amazon Bedrock a chargé un objet dans votre compartiment, la colonne `user_metadata` affiche les métadonnées suivantes associées à cet objet dans le résultat de la requête :

```
user_metadata
{content-additional-params -> requestid="CVK8FWYRW0M9JW65",
 signedContentSHA384="38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe
 content-model-id -> bedrock-model-arn, content-source -> AmazonBedrock}
```

Identification de l'état actuel de vos objets

La requête suivante peut vous aider à déterminer l'état actuel de vos objets. Cette requête identifie la version la plus récente de chaque objet, filtre les objets supprimés et marque la dernière version de chacun d'eux selon des numéros de séquence. Les résultats sont triés en fonction des colonnes `bucket`, `key` et `sequence_number`.

```
WITH records_of_interest as (
   -- Start with a query that can narrow down the records of interest.
    SELECT * from "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal"
),

version_stacks as (
   SELECT *,
```

```
          -- Introduce a column called 'next_sequence_number', which is the next larger
          -- sequence_number for the same key version_id in sorted order.
          LEAD(sequence_number, 1) over (partition by (bucket, key,
 coalesce(version_id, '')) order by sequence_number ASC) as next_sequence_number
   from records_of_interest
),

-- Pick the 'tip' of each version stack triple: (bucket, key, version_id).
-- The tip of the version stack is the row of that triple with the largest sequencer.
-- Selecting only the tip filters out any row duplicates.
-- This isn't typical, but some events can be delivered more than once to the table
-- and include rows that might no longer exist in the bucket (since the
-- table contains rows for both extant and extinct objects).
-- In the next subquery, eliminate the rows that contain deleted objects.
current_versions as (
    SELECT * from version_stacks where next_sequence_number is NULL
),

-- Eliminate the rows that are extinct from the bucket by filtering with
-- record_type. An object version has been deleted from the bucket if its tip is
-- record_type==DELETE.
existing_current_versions as (
    SELECT * from current_versions where not (record_type = 'DELETE' and
 is_delete_marker = FALSE)
),

-- Optionally, to determine which of several object versions is the 'latest',
-- you can compare their sequence numbers. A version_id is the latest if its
-- tip's sequencer is the largest among all other tips in the same key.
with_is_latest as (
    SELECT *,
           -- Determine if the sequence_number of this row is the same as the largest
 sequencer for the key that still exists.
           sequence_number = (MAX(sequence_number) over (partition by (bucket, key)))
 as is_latest_version
    FROM existing_current_versions
)

SELECT * from with_is_latest
ORDER BY bucket, key, sequence_number;
```

Exemples de requêtes de table d'inventaire

Vous pouvez utiliser les exemples de requêtes suivants pour interroger vos tables d'inventaire.

Découvrir les ensembles de données qui utilisent des balises spécifiques

La requête suivante renvoie l'ensemble de données qui utilise les balises spécifiées :

```
SELECT *
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory"
WHERE object_tags['key1'] = 'value1'
AND object_tags['key2'] = 'value2';
```

Répertorier les objets non chiffrés avec SSE-KMS

La requête suivante renvoie des objets qui ne sont pas chiffrés avec SSE-KMS :

```
SELECT key, encryption_status
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory"
WHERE encryption_status != 'SSE-KMS';
```

Répertorier les objets générés par Amazon Bedrock

La requête suivante répertorie les objets générés par Amazon Bedrock :

```
SELECT DISTINCT bucket, key, sequence_number, user_metadata
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory"
WHERE user_metadata['content-source'] = 'AmazonBedrock';
```

Génération de la dernière table d'inventaire

La requête suivante génère la table d'inventaire la plus récente. Cette requête fonctionne lorsque la configuration de vos métadonnées est active. Cette requête nécessite que le journal et les tables d'inventaire soient à l'état Actif. Si votre tableau d'inventaire n'est pas à jour en raison d'autorisations ou d'autres problèmes, cette requête risque de ne pas fonctionner.

Nous recommandons d'utiliser cette requête pour les compartiments à usage général contenant moins d'un milliard d'objets.

Cette requête concilie le contenu de la table d'inventaire avec les événements récents de la table de journal. Lorsque votre journal sera mis à jour avec toutes les modifications apportées à votre compartiment, le résultat de la requête correspondra à celui du contenu du compartiment.

Cet exemple limite la sortie aux seules touches se terminant par`'%.txt'`. Pour interroger un sous-ensemble différent, vous pouvez ajuster l'expression de table commune nommée`"working_set_of_interest"`.

```
WITH inventory_time_cte AS (
    -- Reveal the extent of the journal table that has not yet been reflected in the
 inventory table.
    SELECT COALESCE(inventory_time_from_property, inventory_time_default) AS
 inventory_time FROM
    (
      SELECT * FROM
        -- The fallback default includes the entirety of the journal table.
        (VALUES (TIMESTAMP '2024-12-01 00:00')) AS T (inventory_time_default)
      LEFT OUTER JOIN
        -- This side queries the Iceberg table property and loads it up in
        -- a column. If the property doesn't exist, then you get 0 rows.
        (
         SELECT from_unixtime(CAST(value AS BIGINT)) AS inventory_time_from_property
 FROM "journal$properties"
         WHERE key = 'aws.s3metadata.oldest-uncoalesced-record-timestamp' LIMIT 1
        )
      -- Force an unequivocal join.
      ON TRUE
    )
),

-- Select only those journal table events not yet reflected in the inventory table.
my_new_events AS (
    SELECT journal.* FROM
        (
              journal
            JOIN
              inventory_time_cte
            -- Include only those rows that have yet to be merged with the inventory
 table.
            -- Allow some overlap to account for clock skew.
            ON record_timestamp > (inventory_time - interval '1' hour)
        )
),

-- Bring the "journal" and "inventory" table rows to a common inventory schema.
working_set AS (
    (
        SELECT
            -- Keep the inventory table columns, but drop these journal table columns:
            --   "record_type", "requester", "source_ip_address", "request_id"
            bucket, key, sequence_number,
```

```
            version_id,
            is_delete_marker,
            size,
            COALESCE(last_modified_date, record_timestamp) AS last_modified_date,
            e_tag,
            storage_class,
            is_multipart,
            encryption_status,
            is_bucket_key_enabled,
            kms_key_arn,
            checksum_algorithm,
            object_tags,
            user_metadata,
            -- Temporary columns required to align the two tables.
            record_timestamp AS _log_ts,
            (record_type = 'DELETE' AND NOT COALESCE(is_delete_marker, FALSE)) AS
 _is_perm_delete
        FROM my_new_events
    ) UNION (
            SELECT
                *,
                last_modified_date as _log_ts,
                FALSE AS _is_perm_delete
            FROM "inventory"
    )
),

-- You can apply a filter over key, tags, or metadata here to restrict your view to a
 subset of all keys.
working_set_of_interest AS (
    SELECT * FROM working_set WHERE key LIKE '%.txt'
),

most_recent_changes AS (
  -- For each (bucket, key, version_id) stack, find the event that should have
  -- been the ultimate to arrive in the journal table, and confine the results to the
  -- 1-hour window of events (for that key) that preceded that arrival.
  --
  -- This gives preferential treatment to events that arrived later in the journal
 table
  -- order, and handles cases with uploads that were completed much later after they
 were
  -- initiated.
  SELECT * FROM (
```

```
    SELECT *,
           -- Do not confuse this MAX() with the aggregate function. This is the MAX
 window function.
           MAX(_log_ts) OVER (PARTITION BY bucket, key, version_id) AS _supremum_ts
    FROM working_set_of_interest
  )
  WHERE _log_ts >= (_supremum_ts - interval '1' hour)
),

-- Among each "1-hour window of most recent mutations" for a given key, identify
-- the one that is reflected in the general purpose bucket.
updated_inventory AS (
  SELECT * FROM (
    SELECT *,
           MAX(sequence_number) OVER (PARTITION BY bucket, key, version_id) AS
 _supremum_sn
    FROM most_recent_changes
  )
  WHERE sequence_number = _supremum_sn -- Again here, use QUALIFY clause if your
 planner supports it.
)

-- Finally, project the resulting rows onto the inventory table schema.
SELECT
    bucket,
    key,
    sequence_number,
    version_id,
    is_delete_marker,
    size,
    last_modified_date,
    e_tag,
    storage_class,
    is_multipart,
    encryption_status,
    is_bucket_key_enabled,
    kms_key_arn,
    checksum_algorithm,
    object_tags,
    user_metadata
FROM updated_inventory
WHERE NOT _is_perm_delete
ORDER BY bucket, key ASC, sequence_number ASC
```

Jonction de métadonnées personnalisées à des tables de métadonnées S3

Vous pouvez analyser les données dans vos tables de métadonnées AWS gérées et dans les tables de métadonnées client (autogérées). À l'aide d'un opérateur SQL `JOIN` standard, vous pouvez interroger des données provenant de ces diverses sources.

L'exemple de requête SQL suivant trouve les enregistrements correspondants entre une table de journal AWS gérée (`"journal"`) et une table de métadonnées autogérée (*`my_self_managed_metadata_table`*). La requête filtre également les informations en fonction d'`CREATE`événements, qui indiquent qu'un nouvel objet (ou une nouvelle version de l'objet) a été écrit dans le compartiment. Pour plus d'informations, consultez Schéma des tables de journal des métadonnées S3.

```
SELECT *
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."journal" a
JOIN "my_namespace"."my_self_managed_metadata_table" b
ON a.bucket = b.bucket AND a.key = b.key AND a.version_id = b.version_id
WHERE a.record_type = 'CREATE';
```

L'exemple de requête SQL suivant trouve les enregistrements correspondants entre une table d'inventaire AWS gérée (`"inventory"`) et une table de métadonnées autogérée (*`my_self_managed_metadata_table`*) :

```
SELECT *
FROM "s3tablescatalog/aws-s3"."b_general-purpose-bucket-name"."inventory" a
JOIN "my_namespace"."my_self_managed_metadata_table" b
ON a.bucket = b.bucket AND a.key = b.key AND a.version_id = b.version_id;
```

Visualisation des données des tables de métadonnées avec Amazon QuickSight

Avec Amazon QuickSight, vous pouvez créer des tableaux de bord interactifs pour analyser et visualiser les résultats des requêtes SQL concernant vos tables de métadonnées gérées dans S3. QuickSight les tableaux de bord peuvent vous aider à surveiller les statistiques, à suivre les modifications et à obtenir des informations opérationnelles sur vos tables de métadonnées.

Un tableau de bord concernant le tableau de votre journal peut vous indiquer :

- Quel est le pourcentage de chargements d'objets par rapport aux suppressions ?
- Quels objets ont été supprimés par S3 Lifecycle au cours des dernières 24 heures ?

- De quelles adresses IP proviennent les PUT demandes les plus récentes ?

Un tableau de bord concernant votre tableau d'inventaire peut vous indiquer :

- Combien d'objets se trouvent dans différentes classes de stockage ?
- Quel pourcentage de vos données de stockage est constitué de petits objets par rapport à de grands objets ?
- Quels types d'objets se trouvent dans mon compartiment ?

Après avoir intégré vos compartiments de tables S3 aux services AWS d'analyse, vous pouvez créer des ensembles de données à partir de vos tables de métadonnées et les utiliser dans Amazon QuickSight en utilisant SPICE ou en dirigeant des requêtes SQL depuis votre moteur de requêtes. QuickSight prend en charge Amazon Athena et Amazon Redshift en tant que sources de données.

Pour plus d'informations, consultez Visualiser les données des tables avec Amazon QuickSight.

Résolution des problèmes liés aux métadonnées S3

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation des métadonnées Amazon S3.

Je ne parviens pas à supprimer mon bucket de tables AWS géré et mes tables de métadonnées

Avant de supprimer une table de métadonnées, vous devez commencer par supprimer la configuration de table de métadonnées associée dans votre compartiment à usage général. Pour de plus amples informations, veuillez consulter the section called "Suppression de configurations de tables de métadonnées".

Avant de pouvoir supprimer votre compartiment de table AWS géré, vous devez supprimer toutes les configurations de table de métadonnées associées à ce compartiment ainsi que toutes les tables de métadonnées qu'il contient. Pour plus d'informations, consultez the section called "Suppression de configurations de tables de métadonnées" et the section called "Suppression des tables de métadonnées".

Je ne parviens pas à définir ou à modifier les paramètres de chiffrement pour ma table de métadonnées AWS gérées

Lorsque vous créez la configuration de votre table de métadonnées, vous pouvez choisir de chiffrer vos tables de métadonnées AWS gérées avec un chiffrement côté serveur à l'aide de clés AWS

Key Management Service (AWS KMS) (SSE-KMS). Si vous choisissez d'utiliser SSE-KMS, vous devez fournir une clé KMS gérée par le client dans la même région que votre bucket à usage général. Vous pouvez définir le type de chiffrement de vos tables uniquement lors de leur création. Une fois qu'une table AWS gérée est créée, vous ne pouvez pas modifier ses paramètres de chiffrement. Pour spécifier SSE-KMS pour vos tables de métadonnées, vous devez disposer de certaines autorisations. Pour plus d'informations, consultez la section Autorisations pour SSE-KMS.

Le paramètre de chiffrement d'une table de métadonnées a priorité sur le paramètre de chiffrement par défaut au niveau du compartiment. Si vous ne spécifiez pas de chiffrement pour une table, celle-ci héritera du paramètre de chiffrement par défaut du compartiment.

Par défaut, les compartiments de tables AWS gérés sont chiffrés par chiffrement côté serveur à l'aide de clés gérées Amazon S3 (SSE-S3). Après avoir créé votre première configuration de métadonnées, vous pouvez définir le paramètre de chiffrement par défaut pour le compartiment de table AWS géré afin d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Pour plus d'informations, consultez les sections Chiffrement pour les compartiments de tables AWS gérés etthe section called “Spécification de SSE-KMS”.

Lorsque j'essaie de recréer la configuration de ma table de métadonnées, un message d'erreur s'affiche

La suppression d'une configuration de table de métadonnées entraîne uniquement la suppression de la configuration. Le bucket de table AWS géré et vos tables de métadonnées existent toujours, même si vous supprimez la configuration des tables de métadonnées.

Si vous supprimez la configuration de votre table de métadonnées et souhaitez recréer une configuration pour le même compartiment à usage général, vous devez d'abord supprimer manuellement les anciennes tables de journal et d'inventaire de votre compartiment de tables AWS géré. Dans le cas contraire, la création de la nouvelle configuration de table de métadonnées échoue car ces tables existent déjà.

Pour supprimer vos tables de métadonnées, consultezthe section called “Suppression des tables de métadonnées”.

Je ne parviens pas à activer une table d'inventaire dans ma configuration

Si vous avez créé votre configuration de métadonnées S3 avant le 15 juillet 2025, vous ne pouvez pas activer de table d'inventaire sur cette configuration. Nous vous recommandons de supprimer et de recréer votre configuration afin de pouvoir créer une table d'inventaire et faire expirer les enregistrements des tables de journal. Pour de plus amples informations, veuillez consulter the

section called “Activation des tables d'inventaire sur les configurations de métadonnées créées avant le 15 juillet 2025”.

Je ne parviens pas à activer l'expiration des enregistrements de la table de journal dans ma configuration

Si vous avez créé votre configuration de métadonnées S3 avant le 15 juillet 2025, vous ne pouvez pas activer l'expiration des enregistrements de la table de journal sur cette configuration. Nous vous recommandons de supprimer et de recréer votre configuration afin de pouvoir faire expirer les enregistrements des tables de journal et créer une table d'inventaire. Pour de plus amples informations, veuillez consulter the section called “Activation des tables d'inventaire sur les configurations de métadonnées créées avant le 15 juillet 2025”.

Je ne parviens pas à interroger mes tables de métadonnées

Si vous ne parvenez pas à interroger vos tables de métadonnées, vérifiez les points suivants :

- Lorsque vous utilisez Amazon Athena ou Amazon Redshift pour interroger vos tables de métadonnées, vous devez placer les noms des espaces de noms de vos tables de métadonnées entre guillemets '' () ou backticks ` (), sinon la requête risque de ne pas fonctionner.
- Lorsque vous utilisez Apache Spark Amazon EMR ou d'autres moteurs tiers pour interroger vos tables de métadonnées, nous vous recommandons d'utiliser le point de terminaison Iceberg REST Amazon S3 Tables. Votre requête risque de ne pas s'exécuter correctement si vous n'utilisez pas ce point de terminaison. Pour de plus amples informations, veuillez consulter the section called “Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison”.
- Assurez-vous que vous disposez des autorisations AWS Identity and Access Management (IAM) appropriées pour interroger les tables de métadonnées. Pour de plus amples informations, veuillez consulter the section called “Autorisations pour interroger les tables de métadonnées”.
- Si vous utilisez Amazon Athena et que vous recevez des erreurs lorsque vous essayez d'exécuter vos requêtes, procédez comme suit :
  - Si vous recevez le message d'erreur « Autorisations insuffisantes pour exécuter la requête. Le principal n'a aucun privilège sur la ressource spécifiée. » Lorsque vous essayez d'exécuter une requête dans Athena, vous devez obtenir les autorisations Lake Formation nécessaires sur la table. Pour de plus amples informations, veuillez consulter the section called “Octroi d'une autorisation sur une table ou une base de données”.
  - Si le message d'erreur « Iceberg ne peut pas accéder à la ressource demandée » s'affiche lorsque vous essayez d'exécuter la requête, accédez à la AWS Lake Formation console et assurez-vous que vous vous êtes accordé des autorisations sur le catalogue de compartiments

de tables et la base de données (espace de noms) que vous avez créés. Ne spécifiez pas de table lorsque vous accordez ces autorisations. Pour de plus amples informations, veuillez consulter the section called "Octroi d'une autorisation sur une table ou une base de données".

Je reçois 405 erreurs lorsque j'essaie d'utiliser certaines AWS CLI commandes de métadonnées S3 et certaines opérations d'API

L'appel de l'opération `GetBucketMetadataTableConfiguration` API V1 ou l'utilisation de la commande `get-bucket-metadata-table-configuration` AWS Command Line Interface (AWS CLI) dans le cadre d'une configuration de table de métadonnées V2 entraîne une `405 Method Not Allowed` erreur HTTP. De même, l'appel de l'opération `DeleteBucketMetadataTableConfiguration` API V1 ou l'utilisation de la `delete-bucket-metadata-table-configuration` AWS CLI commande provoque également une erreur 405.

Vous pouvez utiliser l'opération ou la `get-bucket-metadata-configuration` AWS CLI commande de l'`GetBucketMetadataConfiguration`API V2 par rapport à une configuration de table de métadonnées V1 ou V2. De même, vous pouvez utiliser l'opération ou la `delete-bucket-metadata-configuration` AWS CLI commande de l'`DeleteBucketMetadataConfiguration`API V2 par rapport à une configuration de table de métadonnées V1 ou V2.

Nous vous recommandons de mettre à jour vos processus pour utiliser les nouvelles opérations d'API V2 (`CreateBucketMetadataConfigurationGetBucketMetadataConfiguraion`,, et`DeleteBucketMetadataConfiguration`) au lieu des opérations d'API V1. Pour plus d'informations sur la migration de la version V1 de S3 Metadata vers la version V2, consultezthe section called "Activation des tables d'inventaire sur les configurations de métadonnées créées avant le 15 juillet 2025".

Pour déterminer si votre configuration est V1 ou V2, vous pouvez consulter l'attribut suivant de votre réponse d'`GetBucketMetadataConfiguration`API. Un type de compartiment AWS géré (`"aws"`) indique une configuration V2, et un type de compartiment géré par le client (`"customer"`) indique une configuration V1.

```
"MetadataTableConfigurationResult": {
            "TableBucketType": ["aws" | "customer"]
```

Pour de plus amples informations, veuillez consulter the section called "Afficher les configurations des tables de métadonnées".

Chargement d'objets

Lorsque vous chargez un fichier dans Amazon S3, il est stocké en tant qu'objet S3. Les objets se composent des données du fichier et des métadonnées décrivant l'objet. Vous pouvez disposer d'un nombre illimité d'objets dans un compartiment. Avant de pouvoir charger des fichiers dans un compartiment Amazon S3, vous devez disposer d'autorisations en écriture pour le compartiment. Pour plus d'informations sur les autorisations d'accès, consultez Gestion des identités et des accès pour Amazon S3.

Vous pouvez charger n'importe quel type de fichier (images, sauvegardes, données, films, etc.) dans un compartiment S3. La console Amazon S3 vous permet de charger des fichiers d'une taille maximale de 160 Go. Pour charger un fichier de plus de 160 Go, utilisez l'API REST AWS Command Line Interface (AWS CLI) ou Amazon S3. AWS SDKs

Si vous chargez un objet avec un nom de clé qui existe déjà dans un compartiment pour lequel la gestion des versions est activée, Amazon S3 crée une autre version de l'objet au lieu de remplacer l'objet existant. Pour plus d'informations sur l'activation de la gestion des versions, consultez Activation de la gestion des versions sur les compartiments.

Selon la taille des données chargées, Amazon S3 propose les options suivantes :

- Chargez un objet en une seule opération à l' AWS SDKsaide de l'API REST ou AWS CLI : en une seule PUT opération, vous pouvez télécharger un seul objet d'une taille maximale de 5 Go.
- Charger un seul objet à l'aide de la console Amazon S3 : avec la console Amazon S3, vous pouvez charger un seul objet d'une taille maximale de 160 Go.
- Chargez un objet en plusieurs parties à l'aide de l' AWS SDKsAPI REST ou AWS CLI : à l'aide de l'opération d'API de téléchargement en plusieurs parties, vous pouvez télécharger un seul objet de grande taille, d'une taille maximale de 5 To.

  L'opération d'API de chargement partitionné est conçue pour améliorer l'expérience de chargement pour les objets plus volumineux. Vous pouvez charger un objet en plusieurs parties. Ces parties d'objet peuvent être chargées indépendamment, dans n'importe quel ordre, et en parallèle. Vous pouvez utiliser un chargement partitionné pour les objets allant d'une taille maximale de 5 Mo à 5 To. Pour plus d'informations, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Lorsque vous chargez un objet, il est automatiquement chiffré à l'aide du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) par défaut. Lorsque vous le téléchargez, l'objet est

déchiffré. Pour plus d'informations, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3 et Protection des données à l'aide du chiffrement.

Lorsque vous chargez un objet, si vous souhaitez utiliser un autre type de chiffrement par défaut, vous pouvez également spécifier un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) dans vos PUT requêtes S3 ou définir la configuration de chiffrement par défaut dans le compartiment de destination afin d'utiliser SSE-KMS pour chiffrer vos données. Pour en savoir plus sur SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS). Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez avoir l'autorisation d'utiliser la clé. Pour plus d'informations sur les autorisations intercomptes pour les clés KMS, consultez Création de clés KMS que d'autres comptes peuvent utiliser dans le Guide du développeur AWS Key Management Service .

Si vous rencontrez une erreur (403 Forbidden) liée à un refus d'accès dans Amazon S3, consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3 pour en savoir plus sur ses causes courantes.

Charger un objet

Utilisation de la console S3

Cette procédure explique la façon de charger un des objets et des dossiers dans un compartiment Amazon S3 à l'aide de la console.

Lorsque vous chargez un objet, le nom de clé d'objet est le nom du fichier et les préfixes facultatifs. Dans la console Amazon S3, vous pouvez créer des dossiers pour organiser vos objets. Dans Amazon S3, les dossiers sont représentés sous la forme de préfixes qui apparaissent dans le nom de la clé d'objet. Si vous téléchargez un objet individuel dans un dossier de la console Amazon S3, le nom du dossier est inclus dans le nom de la clé de l'objet.

Par exemple, si vous chargez un objet nommé `sample1.jpg` dans un dossier nommé `backup`, le nom de la clé sera `backup/sample1.jpg`. Cependant, l'objet s'affiche dans la console en tant que `sample1.jpg` dans le dossier `backup`. Pour en savoir plus sur les noms de clé, consultez Utilisation des métadonnées d'objet.

> **Note**
>
> Si vous renommez un objet ou modifiez l'une de ses propriétés dans la console Amazon S3, par exemple Classe de stockage, Chiffrement ou Métadonnées, un nouvel objet est créé pour

remplacer l'ancien. Si la gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

Lorsque vous chargez un dossier, Amazon S3 charge tous les fichiers et sous-dossiers du dossier spécifié dans le compartiment. Ensuite, il attribue un nom de clé d'objet qui combine le nom du fichier chargé et le nom du dossier. Par exemple, si vous chargez un dossier nommé `/images` qui contient deux fichiers, `sample1.jpg` et `sample2.jpg`, Amazon S3 charge les fichiers, puis attribue les noms de clé correspondants, `images/sample1.jpg` et `images/sample2.jpg`. Les noms de clé incluent le nom de dossier comme préfixe. La console Amazon S3 affiche uniquement la partie du nom de clé qui suit le dernier signe `/`. Par exemple, dans un dossier `images`, les objets `images/sample1.jpg` et `images/sample2.jpg` s'affichent sous les formes `sample1.jpg` et `sample2.jpg`.

Pour charger des dossiers et des fichiers dans un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment dans lequel vous souhaitez charger vos dossiers ou fichiers.
4. Choisissez Charger.
5. Dans la fenêtre Charger, procédez de l'une des manières suivantes :
   - Faites glisser et déposez les fichiers et les dossiers dans la fenêtre Upload (Charge).
   - Choisissez Ajouter un fichier ou Ajouter un dossier, puis choisissez les fichiers ou les dossiers à charger et Ouvrir.
6. Pour activer la gestion des versions, sous Destination, choisissez Enable Bucket Versioning (Activer la gestion des versions de compartiment).
7. Pour charger les fichiers et les dossiers répertoriés sans configurer des options de chargement supplémentaires, choisissez Charger.

   Amazon S3 charge les objets et les dossiers. Lorsque le chargement est terminé, un message de réussite s'affiche sur la page Charger : statut.

Pour configurer des propriétés d'objet supplémentaires

1. Pour modifier les autorisations de la liste de contrôle d'accès, choisissez Permissions (Autorisations).
2. Sous Access control list (ACL) (Liste de contrôle d'accès (ACL)), modifiez les autorisations.

   Pour plus d'informations sur les autorisations d'accès aux objets, consultez Utilisation de la console S3 pour définir des autorisations ACL pour un objet. Vous pouvez octroyer l'accès en lecture à vos objets au public (tout le monde) pour tous les fichiers que vous chargez. Cependant, nous recommandons de ne pas modifier le paramètre par défaut de l'accès public en lecture. L'octroi de l'accès en lecture public est applicable à un petit sous-ensemble de cas d'utilisation, comme lorsque des compartiments sont utilisés pour des sites web. Vous pouvez toujours modifier les autorisations de l'objet après l'avoir chargé.
3. Pour configurer d'autres propriétés supplémentaires, sélectionnez Properties (Propriétés).
4. Dans Classe de stockage, choisissez la classe de stockage des fichiers à charger.

   Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3.
5. Pour mettre à jour les paramètres de chiffrement de vos objets, sous Server-side encryption settings (Paramètres de chiffrement côté serveur), procédez comme suit.

   a. Choisissez Specify an encryption key (Spécifier une clé de chiffrement).

   b. Sous Paramètres de chiffrement, choisissez Utiliser les paramètres du compartiment pour le chiffrement par défaut ou Ignorer les paramètres du compartiment pour le chiffrement par défaut.

   c. Si vous avez choisi Ignorer les paramètres du compartiment pour le chiffrement par défaut, vous devez configurer les paramètres de chiffrement suivants.

      - Pour chiffrer les fichiers chargés à l'aide des clés gérées par Amazon S3, choisissez Clé gérée par Amazon S3 (SSE-S3).

        Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

      - Pour chiffrer les fichiers téléchargés à l'aide des clés stockées dans AWS Key Management Service (AWS KMS), choisissez AWS Key Management Service key (SSE-KMS). Choisissez ensuite l'une des options suivantes pour CléAWS KMS :

- Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis sélectionnez votre Clé KMS dans la liste des clés disponibles.

  La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

- Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN de votre clé KMS dans le champ qui apparaît.

- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

  Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez d'abord avoir l'autorisation d'utiliser cette clé KMS, puis saisir l'ARN de la clé KMS.
> Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez la section Identifying symmetric and asymmetric KMS keys (Identification des clés KMS symétriques et asymétriques) dans le Guide du développeur AWS Key Management Service .

6. Pour utiliser des sommes de contrôle supplémentaires, sélectionnez Activé. Ensuite, pour le champ Checksum function (Fonction total de contrôle), sélectionnez la fonction que vous souhaitez utiliser. Amazon S3 calcule et stocke la valeur du total de contrôle après avoir reçu l'objet entier. Vous pouvez utiliser la case Precalculated value (Valeur précalculée) pour fournir une valeur précalculée. Si vous le faites, Amazon S3 compare la valeur que vous avez fournie à la valeur qu'il calcule. Si les deux valeurs ne correspondent pas, Amazon S3 génère une erreur.

Les totaux de contrôle supplémentaires vous permettent de spécifier l'algorithme de total de contrôle que vous souhaitez utiliser pour vérifier vos données. Pour plus d'informations sur les totaux de contrôle supplémentaires, consultez Vérification de l'intégrité des objets dans Amazon S3.

7. Pour ajouter des balises à tous les objets que vous chargez, choisissez Add tag (Ajouter une balise). Saisissez un nom de balise dans le champ Clé. Saisissez une valeur pour la balise.

   Le balisage des objets vous permet de classer le stockage par catégorie. Chaque balise est une paire clés-valeurs. Les valeurs de clés et de balises sont sensibles à la casse. Vous pouvez avoir jusqu'à 10 balises par objet. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 255 caractères Unicode. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.

8. Pour ajouter des métadonnées, choisissez Add metadata (Ajouter des métadonnées).

   a. Sous Type, choisissez System defined (Défini par le système) ou User defined (Défini par l'utilisateur).

      Pour les métadonnées définies par le système, vous pouvez sélectionner des en-têtes HTTP courants, tels que Content-Type et Content-Disposition. Pour obtenir la liste des métadonnées définies par le système et savoir si vous pouvez ajouter la valeur, consultez Métadonnées d'objet définies par le système. Toute métadonnée commençant par le préfixe `x-amz-meta-` est traitée comme une métadonnée définie par l'utilisateur. Les métadonnées définies par l'utilisateur sont stockées avec l'objet et renvoyées une fois que vous avez téléchargé l'objet. Les clés et leurs valeurs doivent respecter les normes US-ASCII. Les métadonnées définies par l'utilisateur peuvent atteindre 2 Ko. Pour plus d'informations sur les métadonnées définies par le système et par l'utilisateur, consultez Utilisation des métadonnées d'objet.

   b. Pour Key (Clé), choisissez une clé.

   c. Saisissez une valeur pour la clé.

9. Pour charger vos objets, choisissez Charger.

   Amazon S3 charge votre objet. Lorsque le chargement est terminé, un message de succès s'affiche sur la page Load: status (Charger : statut).

10. Choisissez Exit (Quitter).

À l'aide du AWS CLI

Vous pouvez envoyer une demande PUT pour télécharger un objet d'une taille maximale de 5 Go en une seule opération. Pour plus d'informations, consultez l'exemple `PutObject` dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez envoyer des demandes REST pour charger un objet. Vous pouvez envoyer une demande PUT pour charger des données en une seule opération. Pour plus d'informations, consultez Objet PUT.

À l'aide du AWS SDKs

Vous pouvez utiliser le AWS SDKs pour charger des objets dans Amazon S3. Ils SDKs fournissent des bibliothèques d'encapsulation pour vous permettre de télécharger facilement des données. Pour plus d'informations, consultez la liste des produits pris en charge SDKs.

Voici quelques exemples sélectionnés SDKs :

.NET

L'exemple de code C# crée deux objets avec deux demandes `PutObjectRequest` :

- La première demande `PutObjectRequest`enregistre une chaîne de texte comme exemple de données d'objet. Elle spécifie aussi le nom du compartiment et celui de la clé d'objet.
- La seconde demande `PutObjectRequest` charge un fichier en spécifiant son nom. La demande spécifie aussi l'en-tête `ContentType` et les métadonnées d'objet facultatives (un titre).

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
```

```
{
    class UploadObjectTest
    {
        private const string bucketName = "*** bucket name ***";
        // For simplicity the example creates two objects from the same file.
        // You specify key names for these objects.
        private const string keyName1 = "*** key name for first object created ***";
        private const string keyName2 = "*** key name for second object created
 ***";
        private const string filePath = @"*** file path ***";
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.EUWest1;

        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }

        static async Task WritingAnObjectAsync()
        {
            try
            {
                // 1. Put object-specify only key name for the new object.
                var putRequest1 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName1,
                    ContentBody = "sample text"
                };

                PutObjectResponse response1 = await
 client.PutObjectAsync(putRequest1);

                // 2. Put the object-set ContentType and add metadata.
                var putRequest2 = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName2,
                    FilePath = filePath,
                    ContentType = "text/plain"
                };
```

```
                putRequest2.Metadata.Add("x-amz-meta-title", "someTitle");
                PutObjectResponse response2 = await
 client.PutObjectAsync(putRequest2);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
 object"
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Unknown encountered on server. Message:'{0}' when writing an
 object"
                    , e.Message);
            }
        }
    }
}
```

Java

L'exemple suivant crée deux objets. Le premier objet possède une chaîne de texte comme données et le second objet est un fichier. L'exemple crée le premier objet en spécifiant le nom du compartiment, la clé d'objet et les données de texte directement dans un appel de `AmazonS3Client.putObject()`. L'exemple crée le second objet en utilisant un objet `PutObjectRequest` qui spécifie le nom du compartiment, la clé d'objet et le chemin de fichier. L'objet `PutObjectRequest` spécifie aussi l'en-tête `ContentType` et les métadonnées de titre.

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ObjectMetadata;
import com.amazonaws.services.s3.model.PutObjectRequest;
```

```
import java.io.File;
import java.io.IOException;

public class UploadObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String stringObjKeyName = "*** String object key name ***";
        String fileObjKeyName = "*** File object key name ***";
        String fileName = "*** Path to file to upload ***";

        try {
            // This code expects that you have AWS credentials set up per:
            // https://docs.aws.amazon.com/sdk-for-java/v1/developer-guide/setup-
credentials.html
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .build();

            // Upload a text string as a new object.
            s3Client.putObject(bucketName, stringObjKeyName, "Uploaded String
 Object");

            // Upload a file as a new object with ContentType and title specified.
            PutObjectRequest request = new PutObjectRequest(bucketName,
 fileObjKeyName, new File(fileName));
            ObjectMetadata metadata = new ObjectMetadata();
            metadata.setContentType("plain/text");
            metadata.addUserMetadata("title", "someTitle");
            request.setMetadata(metadata);
            s3Client.putObject(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

JavaScript

L'exemple suivant permet de charger un fichier existant dans un compartiment Amazon S3, dans une région spécifique.

```
import { readFile } from "node:fs/promises";

import {
  PutObjectCommand,
  S3Client,
  S3ServiceException,
} from "@aws-sdk/client-s3";

/**
 * Upload a file to an S3 bucket.
 * @param {{ bucketName: string, key: string, filePath: string }}
 */
export const main = async ({ bucketName, key, filePath }) => {
  const client = new S3Client({});
  const command = new PutObjectCommand({
    Bucket: bucketName,
    Key: key,
    Body: await readFile(filePath),
  });

  try {
    const response = await client.send(command);
    console.log(response);
  } catch (caught) {
    if (
      caught instanceof S3ServiceException &&
      caught.name === "EntityTooLarge"
    ) {
      console.error(
        `Error from S3 while uploading object to ${bucketName}. \
The object was too large. To upload objects larger than 5GB, use the S3 console
 (160GB max) \
or the multipart upload API (5TB max).`,
      );
    } else if (caught instanceof S3ServiceException) {
      console.error(
```

```
        `Error from S3 while uploading object to ${bucketName}.  ${caught.name}:
 ${caught.message}`,
      );
    } else {
      throw caught;
    }
  }
};
```

PHP

Cet exemple vous explique comment utiliser les classes du AWS SDK pour PHP pour télécharger un objet d'une taille maximale de 5 Go. Pour les fichiers plus volumineux, vous devez utiliser l'opération d'API de chargement partitionné. Pour de plus amples informations, veuillez consulter Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

Example — Création d'un objet dans un compartiment Amazon S3 en chargeant des données

L'exemple de code PHP suivant crée un objet dans un compartiment spécifié en chargeant les données grâce à la méthode `putObject()`.

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

try {
    // Upload data.
    $result = $s3->putObject([
        'Bucket' => $bucket,
        'Key'    => $keyname,
        'Body'   => 'Hello, world!',
        'ACL'    => 'public-read'
```

```
    ]);

    // Print the URL to the object.
    echo $result['ObjectURL'] . PHP_EOL;
} catch (S3Exception $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Ruby

La AWS SDK pour Ruby version 3 propose deux méthodes pour télécharger un objet sur Amazon S3. La première utilise un chargeur de fichiers géré, qui simplifie le chargement de fichiers de toute taille à partir du disque. Pour utiliser la méthode de chargeur de fichier géré :

1. Créez une instance de la classe `Aws::S3::Resource`.
2. Référencez l'objet cible grâce au nom du compartiment et à la clé. Les objets résident dans un compartiment et disposent de clés uniques qui identifient chacun d'eux.
3. Appelez`#upload_file` sur l'objet.

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectUploadFileWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Uploads a file to an Amazon S3 object by using a managed uploader.
  #
  # @param file_path [String] The path to the file to upload.
  # @return [Boolean] True when the file is uploaded; otherwise false.
  def upload_file(file_path)
    @object.upload_file(file_path)
    true
  rescue Aws::Errors::ServiceError => e
```

```
    puts "Couldn't upload file #{file_path} to #{@object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-uploaded-file"
  file_path = "object_upload_file.rb"

  wrapper = ObjectUploadFileWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  return unless wrapper.upload_file(file_path)

  puts "File #{file_path} successfully uploaded to #{bucket_name}:#{object_key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

La deuxième méthode utilisée par la AWS SDK pour Ruby version 3 pour télécharger un objet utilise la `#put` méthode de`Aws::S3::Object`. Cela est utile si l'objet est une chaîne ou un I/O objet qui n'est pas un fichier sur le disque. Pour utiliser la méthode :

1. Créez une instance de la classe `Aws::S3::Resource`.
2. Référencez l'objet cible grâce au nom du compartiment et à la clé.
3. Appelez`#put`, en transmettant la chaîne ou I/O l'objet.

Example

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end
```

```
  def put_object(source_file_path)
    File.open(source_file_path, 'rb') do |file|
      @object.put(body: file)
    end
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put #{source_file_path} to #{object.key}. Here's why:
 #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object-key"
  file_path = "my-local-file.txt"

  wrapper = ObjectPutWrapper.new(Aws::S3::Object.new(bucket_name, object_key))
  success = wrapper.put_object(file_path)
  return unless success

  puts "Put file #{file_path} into #{object_key} in #{bucket_name}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Empêcher le chargement d'objets portant des noms de clé identiques

Vous pouvez vérifier l'existence d'un objet dans un compartiment avant de le créer à l'aide d'une écriture conditionnelle lors des opérations de chargement. Cela permet d'éviter l'écrasement de données existantes. Les écritures conditionnelles valident qu'aucun objet portant le même nom de clé ne se trouve déjà dans votre compartiment lors du chargement.

Vous pouvez utiliser des écritures conditionnelles pour les demandes PutObject ou CompleteMultipartUpload.

Pour plus d'informations sur les demandes conditionnelles, consultez Ajout de conditions préalables aux opérations S3 avec des demandes conditionnelles.

Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3

Le chargement partitionné vous permet de charger un seul objet dans Amazon S3 en plusieurs parties. Chaque partie est une portion contiguë des données de l'objet. Vous pouvez charger ces parties d'objet indépendamment et dans n'importe quel ordre. Pour les téléchargements, votre AWS client mis à jour calcule automatiquement la somme de contrôle de l'objet et l'envoie à Amazon S3 avec la taille de l'objet dans le cadre de la demande. Si le transfert d'une partie échoue, vous pouvez la retransférer sans affecter les autres. Une fois que toutes les parties de l'objet sont chargées, Amazon S3 les assemble pour créer cet objet. Il est recommandé d'utiliser le chargement partitionné pour les objets d'au moins 100 Mo au lieu de les charger en une seule opération.

L'utilisation du chargement partitionné offre les avantages suivants :

- Meilleur débit : vous pouvez charger des parties en parallèle pour améliorer le débit.
- Récupération rapide après des problèmes réseau : la taille réduite des parties minimise l'impact du redémarrage d'un chargement qui a échoué en raison d'une erreur de réseau.
- Pause and resume object uploads (Interruption et reprise des chargements d'objet) — vous pouvez charger des parties d'objet au fil du temps. Après le lancement d'un chargement partitionné, il n'y a aucune date d'expiration ; vous devez explicitement le terminer ou l'arrêter.
- Lancement d'un chargement avant de connaître la taille finale de l'objet : vous pouvez charger un objet à mesure que vous le créez.

Nous vous recommandons d'utiliser le chargement partitionné comme suit :

- Si vous chargez des objets volumineux sur un réseau stable à large bande passante, utilisez le chargement partitionné pour optimiser l'utilisation de la bande passante disponible en chargeant plusieurs parties d'objet en parallèle pour bénéficier de performances multithreads.
- Si vous effectuez le chargement sur un réseau irrégulier, utilisez le chargement partitionné pour augmenter la résilience aux erreurs réseau en évitant les redémarrages du chargement. Lorsque vous utilisez le chargement partitionné, vous n'avez besoin de relancer le chargement que pour les parties d'objet dont le chargement a été interrompu. Vous n'avez pas besoin de redémarrer le chargement de vos objets depuis le début.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires. Pour plus d'informations sur l'utilisation du chargement partitionné avec S3 Express One Zone et les compartiments de répertoires, consultez Utilisation du chargement partitionné avec les compartiments de répertoires.

Processus de chargement partitionné

Le chargement partitionné est un processus en trois étapes : vous lancez le chargement, vous chargez les parties de l'objet, et une fois toutes les parties chargées, vous terminez le chargement partitionné. Dès réception de la demande de fin de chargement partitionné, Amazon S3 crée l'objet à partir des parties chargées pour que vous puissiez y accéder comme vous le feriez avec n'importe quel autre objet du compartiment.

Vous pouvez lister tous vos chargements partitionnés en cours ou obtenir une liste des parties que vous avez chargées pour un chargement partitionné spécifique. Chacune de ces opérations est expliquée dans cette section.

Lancement du chargement partitionné

Lorsque vous envoyez une demande pour lancer un chargement partitionné, veillez à spécifier un type de somme de contrôle. Amazon S3 renvoie une réponse avec un ID de chargement, qui est un identifiant unique pour le chargement partitionné. Cet ID de chargement est obligatoire lorsque vous chargez les parties, lorsque vous en affichez la liste, lorsque vous terminez un chargement ou lorsque vous arrêtez un chargement. Si vous souhaitez fournir des métadonnées qui décrivent l'objet en cours de chargement, procédez dans la demande de lancement du chargement partitionné. Les utilisateurs anonymes ne peuvent pas lancer de téléchargements partitionnés.

Chargement de parties

Lorsque vous chargez une partie, outre l'ID de chargement, vous devez spécifier un numéro de partie. Vous pouvez choisir n'importe quel numéro de partie compris entre 1 et 10 000. Un numéro de partie identifie de manière unique une partie et sa place dans l'objet que vous chargez. Le numéro de partie que vous choisissez ne doit pas obligatoirement constituer une séquence consécutive (par exemple, cela peut être 1, 5 et 14). Sachez que si vous chargez une nouvelle partie avec le même numéro qu'une partie précédemment chargée, cette dernière sera écrasée.

Lorsque vous chargez une partie, Amazon S3 renvoie le type d'algorithme de la somme de contrôle avec la valeur de la somme de contrôle pour chaque partie chargée sous forme d'en-tête dans la réponse. Pour chaque téléchargement partiel, vous devez enregistrer le numéro de pièce et la ETag valeur. Vous devez inclure ces valeurs dans la demande ultérieure pour terminer le chargement partitionné. Chaque partie aura la sienne ETag au moment du téléchargement. Cependant, une fois que le téléchargement en plusieurs parties est terminé et que toutes les parties sont consolidées, toutes les parties appartiennent à une seule ETag sous forme de somme de contrôle des sommes de contrôle.

> **Important**
>
> Après avoir lancé un chargement partitionné et après avoir chargé une ou plusieurs parties, vous devez finaliser ou arrêter le chargement partitionné afin que le stockage des parties chargées cesse de vous être facturé. Ce n'est qu'après la fin ou l'arrêt d'un chargement partitionné qu'Amazon S3 libère le stockage des parties et cesse de vous le facturer.
> Après avoir arrêté un chargement partitionné, vous ne pouvez plus charger de partie avec le même ID de chargement. Si des chargements de partie étaient en cours, ils peuvent encore aboutir ou échouer, même après un arrêt du chargement. Pour être sûr de libérer tout le stockage consommé par toutes les parties, n'arrêtez le chargement partitionné qu'après l'aboutissement de tous les chargements partiels.

Fin du chargement partitionné

Lorsque vous terminez un chargement partitionné, Amazon S3 crée un objet en concaténant les parties par ordre croissant en fonction des numéros de partie. Si des métadonnées d'objet sont fournies dans la demande de lancement du chargement partitionné, Amazon S3 les associe à l'objet. À l'issue d'une demande de chargement complet, les parties n'existent plus.

Votre demande complète de téléchargement en plusieurs parties doit inclure l'ID de téléchargement et une liste des numéros de pièce et leurs ETag valeurs correspondantes. La réponse Amazon S3 inclut un ETag identifiant unique les données d'objet combinées. Il ne ETag s'agit pas nécessairement d'un MD5 hachage des données de l'objet.

Lorsque vous fournissez une somme de contrôle complète d'un objet lors d'un chargement en plusieurs parties, le AWS SDK transmet la somme de contrôle à Amazon S3, et S3 valide l'intégrité de l'objet côté serveur, en la comparant à la valeur reçue. S3 stocke ensuite l'objet si les valeurs correspondent. Si les deux valeurs ne correspondent pas, Amazon S3 fait échouer la demande et

génère une erreur `BadDigest`. La somme de contrôle de votre objet est également stockée dans les métadonnées d'objet que vous utiliserez ultérieurement pour valider l'intégrité des données d'un objet.

Exemples d'appels de chargement partitionné

Pour cet exemple, supposons que vous génériez un chargement partitionné pour un fichier de 100 Go. Dans ce cas, vous recevez les appels d'API suivants pour l'ensemble du processus. Il y a un total de 1 002 appels d'API.

- Appel `CreateMultipartUpload` pour commencer le processus.
- 1 000 appels `UploadPart` individuels, chacun chargeant une partie de 100 Mo, pour une taille totale de 100 Go.
- Un appel `CompleteMultipartUpload` pour finaliser le processus.

Listes de chargement partitionné

Vous pouvez lister les parties d'un chargement partitionné spécifique ou de tous les chargements partitionnés en cours. L'opération d'affichage de la liste des parties renvoie des informations sur les parties que vous avez chargées pour un chargement partitionné spécifique. Pour chaque demande de liste des parties, Amazon S3 renvoie des informations sur les parties pour le chargement partitionné spécifié, pour 1 000 parties maximum. S'il y a plus de 1 000 parties dans le chargement partitionné, vous devez envoyer une série de demandes d'affichage des différentes parties chargées pour récupérer toutes les parties. Notez que la liste des parties retournée n'inclut pas les parties qui n'ont pas fini d'être chargées. En utilisant l'opération d'affichage des chargements partitionnés, vous pouvez obtenir la liste des chargements partitionnés qui sont en cours.

Un chargement partitionné en cours est un chargement que vous avez lancé, mais que vous n'avez pas encore terminé ou arrêté. Chaque demande renvoie 1 000 chargements partitionnés maximum. S'il y a plus de 1 000 chargements partitionnés en cours, vous devez envoyer des demandes supplémentaires pour récupérer les chargements partitionnés restants. Utilisez la liste renvoyée uniquement pour la vérification.

> **Important**
>
> N'utilisez pas le résultat de la liste lorsque vous envoyez une requête de chargement partitionné complet. Conservez plutôt votre propre liste des numéros de pièce que vous avez

spécifiés lors du chargement des pièces et des ETag valeurs correspondantes renvoyées par Amazon S3.

Totaux de contrôle avec les opérations de chargement partitionné

Lorsque vous chargez un objet sur Simple Storage Service (Amazon S3), vous pouvez spécifier un algorithme de total de contrôle à utiliser par Amazon S3. Par défaut, le AWS SDK et la console S3 utilisent un algorithme pour tous les téléchargements d'objets, que vous pouvez remplacer. Si vous utilisez un ancien SDK et que votre objet chargé ne possède pas de somme de contrôle spécifiée, Amazon S3 utilise automatiquement l'algorithme de somme de contrôle CRC-64/NVME (). `CRC64NVME` Il s'agit également de l'option recommandée pour une vérification efficace de l'intégrité des données. Lorsque vous utilisez CRC-64/NVME, Amazon S3 calcule la somme de contrôle de l'objet complet une fois le chargement en plusieurs parties ou en une seule partie terminé. L'algorithme de somme de contrôle CRC-64/NVME est utilisé pour calculer soit une somme de contrôle directe de l'objet entier, soit une somme de contrôle des sommes de contrôle, pour chaque partie individuelle.

Une fois que vous avez chargé un objet dans S3 à l'aide du téléchargement partitionné, Amazon S3 calcule la valeur de la somme de contrôle pour chaque partie ou pour l'objet complet et stocke les valeurs. Vous pouvez utiliser l'API ou le AWS SDK S3 pour récupérer la valeur de la somme de contrôle de la manière suivante :

- Pour les parties individuelles, vous pouvez utiliser `GetObject` ou `HeadObject`. Pour récupérer les valeurs des sommes de contrôle pour chaque partie des chargements partitionnés toujours en cours, vous pouvez utiliser `ListParts`.
- Pour l'ensemble de l'objet, vous pouvez utiliser `PutObject`. Si vous souhaitez effectuer un chargement partitionné avec la somme de contrôle d'un objet complet, utilisez `CreateMultipartUpload` et `CompleteMultipartUpload` en spécifiant le type de somme de contrôle de l'objet entier. Pour valider la valeur de la somme de contrôle de l'objet entier ou pour confirmer le type de somme de contrôle utilisé dans le chargement partitionné, utilisez `ListParts`.

> **Important**
>
> Si vous utilisez un téléchargement partitionné avec Checksums, les numéros de pièce pour chaque téléchargement partiel (dans le cas du téléchargement partitionné) doivent utiliser des numéros de pièce consécutifs et commencer par 1. Lorsque vous utilisez des sommes

de contrôle, si vous essayez de finaliser une demande de chargement partitionné avec des numéros de parties non consécutifs, Amazon S3 génère une erreur `HTTP 500 Internal Server`.

Pour plus d'informations sur le fonctionnement des sommes de contrôle avec les objets d'un chargement partitionné, consultez Vérification de l'intégrité des objets dans Amazon S3.

Pour une end-to-end procédure expliquant comment charger un objet à l'aide du téléchargement partitionné avec une somme de contrôle supplémentaire, consultez. Didacticiel : chargement partitionné d'un objet et vérification de l'intégrité de ses données

Opérations simultanées de chargement partitionné

Dans un environnement de développement distribué, il est possible pour l'application de lancer plusieurs mises à jour sur le même objet en même temps. L'application doit lancer plusieurs chargements partitionnés grâce à la même clé d'objet. Pour chacun de ces chargements, l'application peut ensuite charger des parties et envoyer une demande de chargement complet à Amazon S3 pour créer l'objet. Lorsque les compartiments sont activés pour la gestion des versions S3, un chargement partitionné terminé crée toujours une nouvelle version. Lorsque vous lancez plusieurs chargements partitionnés qui utilisent la même clé d'objet dans un compartiment activé pour la gestion des versions, la version actuelle de l'objet est déterminée par le chargement le plus récent (`createdDate`).

Par exemple, vous lancez une demande `CreateMultipartUpload` pour un objet à 10 h. Ensuite, vous soumettez une deuxième demande `CreateMultipartUpload` pour le même objet à 11 h. Comme la deuxième demande a été soumise le plus récemment, l'objet chargé par la demande de 11 h devient la version actuelle, même si le premier chargement se termine après le second. Pour les compartiments pour lesquels la gestion des versions n'a pas été activée, il est possible que d'autres demandes reçues entre le début et la fin d'un chargement partitionné priment.

Un autre exemple de cas où une demande de chargement partitionné simultané peut être prioritaire est le cas d'une autre opération supprimant une clé après que vous avez lancé un chargement partitionné avec cette même clé. Avant que vous ne finalisiez l'opération, la réponse de finalisation du chargement partitionné peut indiquer une création d'objet réussie sans que vous n'ayez jamais vu l'objet.

Empêcher le chargement d'objets portant des noms de clé identiques lors du chargement partitionné

Vous pouvez vérifier l'existence d'un objet dans un compartiment avant de le créer à l'aide d'une écriture conditionnelle lors des opérations de chargement. Cela permet d'éviter l'écrasement de données existantes. Les écritures conditionnelles valident qu'aucun objet portant le même nom de clé ne se trouve déjà dans votre compartiment lors du chargement.

Vous pouvez utiliser des écritures conditionnelles pour les demandes PutObject ou CompleteMultipartUpload.

Pour plus d'informations sur les demandes conditionnelles, consultez Ajout de conditions préalables aux opérations S3 avec des demandes conditionnelles.

Chargement partitionné et tarification

Lorsque vous lancez un chargement partitionné, Amazon S3 conserve toutes les parties jusqu'à ce que vous terminiez ou arrêtiez le chargement. Tout au long de sa durée de vie, le stockage, la bande passante et les demandes pour ce chargement partitionné ainsi que ses parties associées vous sont facturés.

Ces parties sont facturées en fonction de la classe de stockage spécifiée lors du chargement des parties. Toutefois, ces parties ne vous seront pas facturées si elles sont chargées dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Les parties multipartites en cours d'exécution d'une commande PUT vers la classe de stockage S3 Glacier Flexible Retrieval sont facturées en tant que stockage de transit S3 Glacier Flexible Retrieval aux tarifs de stockage S3 Standard jusqu'à ce que le chargement soit terminé. De plus, `CreateMultipartUpload` et `UploadPart` sont tous deux facturés aux tarifs S3 Standard. Seule la demande `CompleteMultipartUpload` est facturée au tarif S3 Glacier Flexible Retrieval. De même, les parties multipartites en cours d'exécution d'une commande PUT vers la classe de stockage S3 Glacier Deep Archive sont facturées en tant que stockage de transit S3 Glacier Flexible Retrieval aux tarifs de stockage standard S3 jusqu'à ce que le chargement soit terminé. Seule la demande `CompleteMultipartUpload` est facturée aux tarifs S3 Glacier Deep Archive.

Si vous arrêtez le chargement partitionné, Amazon S3 supprime les artefacts et toutes les parties que vous avez chargées. Ces artefacts ne vous seront pas facturés. Aucuns frais de suppression anticipée ne sont facturés pour la suppression de chargements partitionnés incomplets, quelle que soit la classe de stockage spécifiée. Pour plus d'informations sur la tarification, consultez Tarification Amazon S3.

> **Note**
>
> Pour réduire vos coûts de stockage, nous vous recommandons de configurer une règle du cycle de vie pour supprimer les chargements partitionnés incomplets après un certain nombre de jours à l'aide de l'action `AbortIncompleteMultipartUpload`. Pour plus d'informations sur la création d'une règle de cycle de vie pour supprimer les chargements partitionnés incomplets, consultez Configuration d'une politique de cycle de vie de compartiment pour abandonner les chargements multiparties incomplets.

Prise en charge de l'API pour le chargement partitionné

Les sections suivantes de la Référence de l'API Amazon Simple Storage Service décrivent l'API REST pour le chargement partitionné.

Pour une procédure de téléchargement en plusieurs parties utilisant les fonctions AWS Lambda, consultez la section Chargement d'objets volumineux sur Amazon S3 à l'aide du chargement en plusieurs parties et de l'accélération du transfert.

- Création d'un chargement partitionné
- Chargement d'une partie
- Chargement d'une partie (Copy)
- Achèvement du chargement partitionné
- Interruption du chargement partitionné
- Liste des parties
- Liste des chargements partitionnés

AWS Command Line Interface support pour le téléchargement partitionné

Les rubriques suivantes AWS Command Line Interface décrivent les opérations de téléchargement partitionné.

- Lancement du chargement partitionné
- Chargement d'une partie
- Chargement d'une partie (Copy)
- Achèvement du chargement partitionné

- Interruption du chargement partitionné
- Liste des parties
- Liste des chargements partitionnés

AWS Support du SDK pour le téléchargement en plusieurs parties

Vous pouvez utiliser an AWS SDKs pour télécharger un objet en plusieurs parties. Pour une liste des actions AWS SDKs prises en charge par l'API, voir :

- Création d'un chargement partitionné
- Chargement d'une partie
- Chargement d'une partie (Copy)
- Achèvement du chargement partitionné
- Interruption du chargement partitionné
- Liste des parties
- Liste des chargements partitionnés

API de chargement partitionné et autorisations

Vous devez posséder les autorisations nécessaires pour utiliser les opérations de chargement partitionné. Vous pouvez utiliser les listes de contrôle d'accès (ACLs), la politique des compartiments ou la politique utilisateur pour autoriser les individus à effectuer ces opérations. Le tableau suivant répertorie les autorisations requises pour les différentes opérations de téléchargement partitionné lors de l'utilisation ACLs d'une politique de compartiment ou d'une politique utilisateur.

Action	Autorisations requises
Création d'un chargement partitionné	Vous devez être autorisé à exécuter l'action `s3:PutObject` sur un objet pour pouvoir créer un chargement partitionné. Le propriétaire du compartiment peut autoriser d'autres personnes habilitées à exécuter l'action `s3:PutObject` .
Lancement du	Vous devez être autorisé à exécuter l'action `s3:PutObject` sur un objet pour pouvoir lancer le chargement partitionné.

Action	Autorisations requises
chargement partitionné	Le propriétaire du compartiment peut autoriser d'autres personnes habilitées à exécuter l'action `s3:PutObject` .
Initiateur	Elément du conteneur qui identifie l'initiateur du chargement partitionné. Si l'initiateur est un Compte AWS, cet élément fournit les mêmes informations que l'élément Owner. Si l'initiateur est un utilisateur IAM, cet élément fournit l'ARN utilisateur et le nom complet.
Chargement d'une partie	Vous devez être autorisé à exécuter l'action `s3:PutObject` sur un objet pour charger une partie. Le propriétaire du compartiment doit autoriser l'initiateur à exécuter l'action `s3:PutObject` sur un objet pour que ce dernier charge une partie pour cet objet.
Chargement d'une partie (Copy)	Vous devez être autorisé à exécuter l'action `s3:PutObject` sur un objet pour charger une partie. Sachant que vous chargez une partie d'un objet existant, vous devez être autorisé à exécuter l'action `s3:GetObject` sur l'objet source. Pour que l'initiateur puisse charger une partie pour un objet, le propriétaire du compartiment doit l'autoriser à effectuer l'action `s3:PutObject` sur l'objet.
Achèvement du chargement partitionné	Vous devez être autorisé à exécuter l'action `s3:PutObject` sur un objet pour terminer le chargement partitionné. Le propriétaire du compartiment doit autoriser l'initiateur à exécuter l'action `s3:PutObject` sur un objet pour que ce dernier termine un chargement partitionné pour cet objet.

Action	Autorisations requises
Arrêt du chargement partitionné	Vous devez être autorisé à exécuter l'action `s3:AbortMultipartUpload` pour arrêter un chargement partitionné. Par défaut, le propriétaire du compartiment et l'initiateur du chargement partitionné sont autorisés à exécuter cette action dans le cadre des politiques IAM et de compartiment S3. Si l'initiateur est un utilisateur IAM, celui-ci Compte AWS est également autorisé à arrêter ce téléchargement partitionné. Dans le cadre des politiques de point de terminaison de VPC, l'initiateur du chargement partitionné n'a pas automatiquement l'autorisation d'effectuer l'action `s3:AbortMultipartUpload` . Outre ces paramètres par défaut, le propriétaire du compartiment peut autoriser d'autres principaux à être habilité à exécuter l'action `s3:AbortMultipartUpload` sur un objet. Le propriétaire du compartiment peut refuser que tout principal soit habilité à exécuter l'action `s3:AbortMultipartUpload` .
Liste des parties	Vous devez être autorisé à exécuter l'action `s3:ListMultipartUploadParts` sur un objet pour lister les parties lors d'un chargement partitionné. Par défaut, le propriétaire du compartiment est autorisé à lister les parties pour tout chargement partitionné dans le compartiment. L'initiateur du chargement partitionné est autorisé à lister les parties du chargement partitionné spécifique. Si l'initiateur du téléchargement partitionné est un utilisateur IAM, l'utilisateur IAM Compte AWS contrôlant cet utilisateur est également autorisé à répertorier les parties de ce téléchargement. Outre ces paramètres par défaut, le propriétaire du compartiment peut autoriser d'autres principaux à être habilité à exécuter l'action `s3:ListMultipartUploadParts` sur un objet. Le propriétaire du compartiment peut également refuser que tout principal soit habilité à exécuter l'action `s3:ListMultipartUploadParts` .

Action	Autorisations requises
Liste des chargements partitionnés	Vous devez être autorisé à exécuter l'action `s3:ListBucketMultipartUploads` sur un compartiment pour lister les chargements partitionnés en cours dans ce compartiment. Outre ces paramètres par défaut, le propriétaire du compartiment peut autoriser d'autres personnes habilitées à exécuter l'action `s3:ListBucketMultipartUploads` sur le compartiment.
AWS KMS Chiffrer et déchiffrer les autorisations associées	Pour effectuer un téléchargement partitionné avec chiffrement à l'aide d'une clé KMS AWS Key Management Service (AWS KMS), le demandeur doit disposer des autorisations suivantes : • Actions `kms:Decrypt` et `kms:GenerateDataKey` au niveau de la clé • Action `kms:GenerateDataKey` pour l'API CreateMultipartUpload • L'`kms:Decrypt` action sur le UploadPartterrain UploadPartCopy APIs. Ces autorisations sont requises, car Simple Storage Service (Amazon S3) doit déchiffrer et lire les données des parties de fichier chiffrées avant de terminer le chargement partitionné. L'autorisation `kms:Decrypt` et le chiffrement côté serveur avec les clés de chiffrement fournies par le client sont également nécessaires pour obtenir la valeur de la somme de contrôle d'un objet. Si vous ne disposez pas des autorisations requises lorsque vous utilisez l'API CompleteMultipartUpload, l'objet sera créé sans valeur de somme de contrôle. Si votre utilisateur ou rôle IAM est identique Compte AWS à celui de la clé KMS, vérifiez que vous disposez d'autorisations à la fois sur la clé et sur les politiques IAM. Si votre utilisateur ou rôle IAM appartient à un autre compte que la clé KMS, vous devez disposer des autorisations sur la politique de clé et votre utilisateur ou rôle IAM.

Action	Autorisations requises
SSE-C (chiffrement côté serveur à l'aide des clés de chiffrement fournies par le client)	Lorsque vous utilisez l'API CompleteMultipartUpload, vous devez fournir un chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C). Dans le cas contraire, l'objet sera créé sans somme de contrôle et aucune valeur de somme de contrôle ne sera renvoyée.

Pour en savoir plus sur la relation entre les autorisations de liste ACL et les autorisations des politiques d'accès, consultez Mappage des autorisations de liste ACL et de stratégie d'accès. Pour obtenir plus d'informations sur les utilisateurs IAM, les rôles et les bonnes pratiques, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles) dans le Guide de l'utilisateur IAM.

Totaux de contrôle avec les opérations de chargement partitionné

Trois Amazon S3 APIs sont utilisés pour effectuer le chargement partitionné proprement dit : `CreateMultipartUpload`, `UploadPart`, et `CompleteMultipartUpload`. Le tableau suivant indique les en-têtes et les valeurs de checksum qui doivent être fournis pour chacun des éléments : APIs

Algorithme de somme de contrôle	Type de somme de contrôle	**CreateMultipartUpload**	**UploadPart**	**CompleteMultipartUpload**

CRC-64/NVME () `CRC64NVME`	Objet complet	En-têtes obligatoires :
		`x-amz-checksum-algorithm`
			En-têtes facultatifs :
			`x-amz-checksum-crc64nvme`
				En-têtes facultatifs :
				`x-amz-checksum-algorithm`
				`x-amz-crc64`

CRC-32 () `CRC32`	Objet complet	En-têtes obligatoires :	En-têtes facultatifs :	En-têtes facultatifs :

Algorithme de somme de contrôle	Type de somme de contrôle	**CreateMultipartUpload**	**UploadPart**	**CompleteMultipartUpoad**

CRTC 32-C () CRC32C		`x-amz-checksum-algorithm`
		
		`x-amz-checksum-type`
			`x-amz-checksum-crc64nvme`	`x-amz-checksum-algorithm`
				
				`x-amz-crc32`
				
				`x-amz-crc32c`

Algorithme de somme de contrôle	Type de somme de contrôle	**CreateMultipartUpload**	**UploadPart**	**CompleteMultipartUpload**

CRC-32 () `CRC32`
 	
CRC-32C () `CRC32C`
 	
SHA-1 () `SHA1`
 	
SHA-256 () `SHA256`
	Composite	En-têtes obligatoires :
		
		`x-amz-checksum-algorithm`
			En-têtes obligatoires :
			
			`x-amz-checksum-crc32`
			
			`x-amz-checksum-crc32c`
			
			`x-amz-checksum-sha1`
			
			`x-amz-checksum-sha256`
				En-têtes obligatoires :
				
				Toutes les sommes de contrôle au niveau de chaque partie doivent être incluses dans la demande `CompleteMultiPartUpload` .
				
				En-têtes facultatifs :
				
				`x-amz-crc32`
				
				`x-amz-crc32c`
				
				`x-amz-sha1`
				
				`x-amz-sha256`

Rubriques

- Configuration d'une configuration de cycle de vie de compartiment pour supprimer les chargements partitionnés incomplets
- Chargement d'un objet à l'aide du chargement partitionné
- Chargement d'un répertoire à l'aide de la classe TransferUtility .

- Liste des chargements partitionnés
- Suivi d'un téléchargement en plusieurs parties à l'aide du AWS SDKs
- Interruption d'un chargement partitionné
- Copie d'un objet à l'aide du chargement partitionné
- Didacticiel : chargement partitionné d'un objet et vérification de l'intégrité de ses données
- Limites de la fonction de chargement partitionné Amazon S3

Configuration d'une configuration de cycle de vie de compartiment pour supprimer les chargements partitionnés incomplets

Dans le cadre des bonnes pratiques, nous vous recommandons de configurer une règle du cycle de vie à l'aide de l'action `AbortIncompleteMultipartUpload` pour réduire les coûts de stockage. Pour plus d'informations sur l'abandon d'un chargement multipartie, consultez Interruption d'un chargement partitionné.

Simple Storage Service (Amazon S3) prend en charge une règle de cycle de vie de compartiment que vous pouvez utiliser pour demander à Simple Storage Service (Amazon S3) d'arrêter les chargements partitionnés s'ils ne se terminent pas avant la valeur spécifiée pour le nombre de jours après leur lancement. Lorsqu'un chargement partitionné n'est pas terminé dans le délai imparti, il peut être annulé. Amazon S3 arrête alors le chargement partitionné et supprime les pièces associées au chargement partitionné. Cette règle s'applique à la fois aux chargements partitionnés existants et à ceux que vous créerez ultérieurement.

Voici un exemple de configuration du cycle de vie qui spécifie une règle avec l'action `AbortIncompleteMultipartUpload`.

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Prefix></Prefix>
        <Status>Enabled</Status>
        <AbortIncompleteMultipartUpload>
          <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
</LifecycleConfiguration>
```

Dans l'exemple, la règle ne spécifie pas de valeur pour l'élément `Prefix` (le préfixe du nom de la clé de l'objet). Par conséquent, la règle s'applique à tous les objets du compartiment pour lesquels vous avez lancé des téléchargements partitionnés. Tous les téléchargements partitionnés qui ont été lancés et qui ne se sont pas terminés dans les sept jours peuvent faire l'objet d'une interruption. L'action Annuler n'a aucun effet sur les téléchargements partitionnés terminés.

Pour en savoir plus sur la configuration du cycle de vie du compartiment, consultez Gestion du cycle de vie des objets.

> **Note**
>
> Si le chargement partitionné est terminé dans le temps imparti spécifié dans la règle, l'action du cycle de vie `AbortIncompleteMultipartUpload` ne s'applique pas (cela signifie qu'Amazon S3 n'applique aucune action). En outre, cette action ne s'applique pas aux objets. Aucun objet n'est supprimé par cette action de cycle de vie. De plus, vous n'aurez pas à payer de frais de suppression anticipée pour le cycle de vie S3 lorsque vous supprimez des parties de chargements partitionnés incomplets.

Utilisation de la console S3

Pour gérer automatiquement les chargements partitionnés incomplets, vous pouvez utiliser la console S3 pour créer une règle de cycle de vie afin de faire expirer les octets de chargement partitionnés incomplets de votre compartiment après un nombre de jours spécifié. La procédure suivante vous montre comment ajouter une règle de cycle de vie pour supprimer les chargements partitionnés incomplets après sept jours. Pour plus d'informations sur l'ajout de règles de cycle de vie, consultez Définition d'une configuration du cycle de vie S3 sur un compartiment.

Pour ajouter une règle de cycle de vie afin d'interrompre les chargements partitionnés incomplets datant de plus de sept jours.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le nom du compartiment pour lequel vous souhaitez créer une stratégie de cycle de vie.
3. Choisissez l'onglet Management (Gestion), puis choisissez Create lifecycle rule (Créer une règle de cycle de vie).
4. Dans Lifecycle rule name (Nom de la règle du cycle de vie), saisissez un nom pour votre règle.

Ce nom doit être unique dans le compartiment.

5. Choisissez l'étendue de la règle de cycle de vie :

   - Pour créer une règle de cycle de vie pour tous les objets ayant un préfixe spécifique, sélectionnez Limit the scope of this rule using one or more filters (Limiter l'étendue de cette règle à l'aide d'un ou plusieurs filtres), puis saisissez le préfixe dans le champ Prefix (Préfixe).
   - Pour créer une règle de cycle de vie pour tous les objets du compartiment, sélectionnez l'option This rule applies to all objects in the bucket (Cette règle s'applique à tous les objets du compartiment), puis sélectionnez I acknowledge that this rule applies to all objects in the bucket (Je reconnais que cette règle s'applique à tous les objets du compartiment).

6. Sous Lifecycle rule actions (Actions des règles de cycle de vie), sélectionnez Delete expired object delete markers or incomplete multipart uploads (Supprimer les marqueurs de suppression d'objets expirés ou les chargements partitionnés incomplets).
7. Sous Delete expired object delete markers or incomplete multipart uploads (Supprimer les marqueurs de suppression des objets expirés ou les chargements partitionnés incomplets), sélectionnez Delete incomplete multipart uploads (Supprimer les chargements partitionnés incomplets).
8. Dans le champ Number of days (Nombre de jours), saisissez le nombre de jours au bout duquel vous souhaitez supprimer les chargements partitionnés incomplets (dans cet exemple, sept jours).
9. Choisissez Créer une règle.

À l'aide du AWS CLI

La commande suivante `put-bucket-lifecycle-configuration`AWS Command Line Interface (AWS CLI) ajoute la configuration du cycle de vie pour le compartiment spécifié. Pour utiliser cette commande, remplacez *`user input placeholders`* par vos informations.

```
aws s3api put-bucket-lifecycle-configuration  \
        --bucket amzn-s3-demo-bucket  \
        --lifecycle-configuration filename-containing-lifecycle-configuration
```

L'exemple suivant montre comment ajouter une règle de cycle de vie pour interrompre les chargements partitionnés incomplets en utilisant la AWS CLI. Il comprend un exemple de configuration du cycle de vie JSON pour interrompre les chargements partitionnés incomplets datant de plus de sept jours.

Pour utiliser les commandes CLI de cet exemple, remplacez *user input placeholders* par vos informations.

Pour ajouter une règle de cycle de vie afin d'interrompre les chargements partitionnés incomplets

1. Configurez le AWS CLI. Pour obtenir des instructions, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.
2. Enregistrez l'exemple de configuration du cycle de vie suivant dans un fichier (par exemple, *lifecycle.json*). Cet exemple de configuration spécifie un préfixe vide, et s'applique donc à tous les objets du compartiment. Pour restreindre la configuration à un sous-ensemble d'objets, vous pouvez spécifier un préfixe.

```
{
    "Rules": [
        {
            "ID": "Test Rule",
            "Status": "Enabled",
            "Filter": {
                "Prefix": ""
            },
            "AbortIncompleteMultipartUpload": {
                "DaysAfterInitiation": 7
            }
        }
    ]
}
```

3. Exécutez la commande CLI suivante pour configurer cette configuration du cycle de vie sur le compartiment.

```
aws s3api put-bucket-lifecycle-configuration   \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

4. Pour vérifier que la configuration du cycle de vie a été définie sur votre compartiment, récupérez la configuration du cycle de vie en utilisant la commande `get-bucket-lifecycle` suivante.

```
aws s3api get-bucket-lifecycle  \
--bucket amzn-s3-demo-bucket
```

5. Pour supprimer la configuration du cycle de vie, utilisez la commande `delete-bucket-lifecycle` suivante.

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

Chargement d'un objet à l'aide du chargement partitionné

Vous pouvez utiliser le chargement partitionné pour charger par programme un seul objet sur Amazon S3. Chaque objet est chargé en tant qu'ensemble de parties. Chaque partie est une portion contiguë des données de l'objet. Vous pouvez charger ces parties d'objet indépendamment et dans n'importe quel ordre. Si le transfert d'une partie échoue, vous pouvez la retransférer sans affecter les autres. Une fois toutes les parties de l'objet chargées, Amazon S3 les assemble et crée l'objet. Les utilisateurs anonymes ne peuvent pas lancer de téléchargements partitionnés.

Pour une end-to-end procédure de téléchargement d'un objet avec un téléchargement en plusieurs parties avec une somme de contrôle supplémentaire, voir. Didacticiel : chargement partitionné d'un objet et vérification de l'intégrité de ses données

La section suivante explique comment utiliser le téléchargement partitionné avec le AWS Command Line Interface, et AWS SDKs.

Utilisation de la console S3

Vous pouvez charger n'importe quel type de fichier (images, sauvegardes, données, films, etc.) dans un compartiment S3. La console Amazon S3 vous permet de charger des fichiers d'une taille maximale de 160 Go. Pour charger un fichier de plus de 160 Go, utilisez l'API REST AWS Command Line Interface (AWS CLI) ou Amazon S3. AWS SDKs

Pour obtenir des instructions sur le téléchargement d'un objet via le AWS Management Console, consultezChargement d'objets.

À l'aide du AWS CLI

La section suivante décrit les opérations Amazon S3 pour le chargement partitionné à l'aide de l' AWS CLI.

- Lancement du chargement partitionné
- Chargement d'une partie

- Chargement d'une partie (Copy)
- Achèvement du chargement partitionné
- Interruption du chargement partitionné
- Liste des parties
- Liste des chargements partitionnés

Utilisation de l'API REST

Les sections suivantes de la Référence de l'API Amazon Simple Storage Service décrivent l'API REST pour le chargement partitionné.

- Lancement du chargement partitionné
- Chargement d'une partie
- Achèvement du chargement partitionné
- Arrêt du chargement partitionné
- Liste des parties
- Liste des chargements partitionnés

Utilisation de AWS SDKs (API de haut niveau)

Certains AWS SDKs proposent une API de haut niveau qui simplifie le téléchargement en plusieurs parties en combinant les différentes opérations d'API requises pour effectuer un téléchargement en plusieurs parties en une seule opération. Pour de plus amples informations, veuillez consulter Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Si vous devez interrompre et reprendre des chargements partitionnés, modifiez la taille des parties lors du chargement, ou si vous ignorez la taille des données à charger, utilisez les méthodes d'API de bas niveau. Les méthodes d'API de bas niveau pour les chargements partitionnés offrent des fonctionnalités supplémentaires. Pour plus d'informations, consultez Utilisation de AWS SDKs (API de bas niveau).

.NET

Pour charger un fichier dans un compartiment S3, utilisez la classe `TransferUtility`. Lorsque vous chargez les données d'un fichier, vous devez fournir le nom de clé de l'objet. Sinon, l'API

utilise le nom du fichier comme nom de clé. Lorsque vous chargez les données d'un flux, vous devez fournir le nom de clé de l'objet.

Utilisez la classe `TransferUtilityUploadRequest` pour définir des options avancées, comme la taille des parties, le nombre de threads lors du chargement simultané des parties, les métadonnées, la classe de stockage ou une liste ACL.

> **Note**
>
> Lorsque vous utilisez un flux comme source de données, la classe `TransferUtility` n'effectue pas de chargements simultanés.

L'exemple C# suivant charge un fichier dans un compartiment Amazon S3 en plusieurs parties. Il montre comment utiliser différentes surcharges `TransferUtility.Upload` pour charger un fichier. Chaque appel de chargement successif remplace le chargement précédent. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPUHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
```

```
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadFileAsync().Wait();
        }

        private static async Task UploadFileAsync()
        {
            try
            {
                var fileTransferUtility =
                    new TransferUtility(s3Client);

                // Option 1. Upload a file. The file name is used as the object key
name.
                await fileTransferUtility.UploadAsync(filePath, bucketName);
                Console.WriteLine("Upload 1 completed");

                // Option 2. Specify object key name explicitly.
                await fileTransferUtility.UploadAsync(filePath, bucketName,
keyName);
                Console.WriteLine("Upload 2 completed");

                // Option 3. Upload data from a type of System.IO.Stream.
                using (var fileToUpload =
                    new FileStream(filePath, FileMode.Open, FileAccess.Read))
                {
                    await fileTransferUtility.UploadAsync(fileToUpload,
                                               bucketName, keyName);
                }
                Console.WriteLine("Upload 3 completed");

                // Option 4. Specify advanced settings.
                var fileTransferUtilityRequest = new TransferUtilityUploadRequest
                {
                    BucketName = bucketName,
                    FilePath = filePath,
                    StorageClass = S3StorageClass.StandardInfrequentAccess,
                    PartSize = 6291456, // 6 MB.
                    Key = keyName,
                    CannedACL = S3CannedACL.PublicRead
                };
                fileTransferUtilityRequest.Metadata.Add("param1", "Value1");
                fileTransferUtilityRequest.Metadata.Add("param2", "Value2");
```

```
                await fileTransferUtility.UploadAsync(fileTransferUtilityRequest);
                Console.WriteLine("Upload 4 completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }

        }
    }
}
```

JavaScript

Example

Chargez un fichier volumineux.

```
import { S3Client } from "@aws-sdk/client-s3";
import { Upload } from "@aws-sdk/lib-storage";

import {
  ProgressBar,
  logger,
} from "@aws-doc-sdk-examples/lib/utils/util-log.js";

const twentyFiveMB = 25 * 1024 * 1024;

export const createString = (size = twentyFiveMB) => {
  return "x".repeat(size);
};

/**
 * Create a 25MB file and upload it in parts to the specified
 * Amazon S3 bucket.
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
```

```
  const str = createString();
  const buffer = Buffer.from(str, "utf8");
  const progressBar = new ProgressBar({
    description: `Uploading "${key}" to "${bucketName}"`,
    barLength: 30,
  });

  try {
    const upload = new Upload({
      client: new S3Client({}),
      params: {
        Bucket: bucketName,
        Key: key,
        Body: buffer,
      },
    });

    upload.on("httpUploadProgress", ({ loaded, total }) => {
      progressBar.update({ current: loaded, total });
    });

    await upload.done();
  } catch (caught) {
    if (caught instanceof Error && caught.name === "AbortError") {
      logger.error(`Multipart upload was aborted. ${caught.message}`);
    } else {
      throw caught;
    }
  }
};
```

Example

Téléchargez un fichier volumineux.

```
import { fileURLToPath } from "node:url";
import { GetObjectCommand, NoSuchKey, S3Client } from "@aws-sdk/client-s3";
import { createWriteStream, rmSync } from "node:fs";

const s3Client = new S3Client({});
const oneMB = 1024 * 1024;

export const getObjectRange = ({ bucket, key, start, end }) => {
```

```
  const command = new GetObjectCommand({
    Bucket: bucket,
    Key: key,
    Range: `bytes=${start}-${end}`,
  });

  return s3Client.send(command);
};

/**
 * @param {string | undefined} contentRange
 */
export const getRangeAndLength = (contentRange) => {
  const [range, length] = contentRange.split("/");
  const [start, end] = range.split("-");
  return {
    start: Number.parseInt(start),
    end: Number.parseInt(end),
    length: Number.parseInt(length),
  };
};

export const isComplete = ({ end, length }) => end === length - 1;

const downloadInChunks = async ({ bucket, key }) => {
  const writeStream = createWriteStream(
    fileURLToPath(new URL(`./${key}`, import.meta.url)),
  ).on("error", (err) => console.error(err));

  let rangeAndLength = { start: -1, end: -1, length: -1 };

  while (!isComplete(rangeAndLength)) {
    const { end } = rangeAndLength;
    const nextRange = { start: end + 1, end: end + oneMB };

    const { ContentRange, Body } = await getObjectRange({
      bucket,
      key,
      ...nextRange,
    });
    console.log(`Downloaded bytes ${nextRange.start} to ${nextRange.end}`);

    writeStream.write(await Body.transformToByteArray());
    rangeAndLength = getRangeAndLength(ContentRange);
```

```
  }
};

/**
 * Download a large object from and Amazon S3 bucket.
 *
 * When downloading a large file, you might want to break it down into
 * smaller pieces. Amazon S3 accepts a Range header to specify the start
 * and end of the byte range to be downloaded.
 *
 * @param {{ bucketName: string, key: string }}
 */
export const main = async ({ bucketName, key }) => {
  try {
    await downloadInChunks({
      bucket: bucketName,
      key: key,
    });
  } catch (caught) {
    if (caught instanceof NoSuchKey) {
      console.error(`Failed to download object. No such key "${key}".`);
      rmSync(key);
    }
  }
};
```

Go

Pour plus d'informations sur l'exemple de code Go pour le chargement en plusieurs parties, consultez Charger ou télécharger des fichiers volumineux vers et depuis Amazon S3 à l'aide d'un AWS SDK.

Example

Chargez un objet volumineux à l'aide d'un gestionnaire de chargement qui divise les données en plusieurs parties et les charge simultanément.

```
import (
 "bytes"
 "context"
 "errors"
 "fmt"
```

```
 "io"
 "log"
 "os"
 "time"

 "github.com/aws/aws-sdk-go-v2/aws"
 "github.com/aws/aws-sdk-go-v2/feature/s3/manager"
 "github.com/aws/aws-sdk-go-v2/service/s3"
 "github.com/aws/aws-sdk-go-v2/service/s3/types"
 "github.com/aws/smithy-go"
)

// BucketBasics encapsulates the Amazon Simple Storage Service (Amazon S3) actions
// used in the examples.
// It contains S3Client, an Amazon S3 service client that is used to perform bucket
// and object actions.
type BucketBasics struct {
 S3Client *s3.Client
}
```

```
// UploadLargeObject uses an upload manager to upload data to an object in a bucket.
// The upload manager breaks large data into parts and uploads the parts
 concurrently.
func (basics BucketBasics) UploadLargeObject(ctx context.Context, bucketName string,
 objectKey string, largeObject []byte) error {
 largeBuffer := bytes.NewReader(largeObject)
 var partMiBs int64 = 10
 uploader := manager.NewUploader(basics.S3Client, func(u *manager.Uploader) {
  u.PartSize = partMiBs * 1024 * 1024
 })
 _, err := uploader.Upload(ctx, &s3.PutObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
  Body:   largeBuffer,
 })
 if err != nil {
  var apiErr smithy.APIError
  if errors.As(err, &apiErr) && apiErr.ErrorCode() == "EntityTooLarge" {
   log.Printf("Error while uploading object to %s. The object is too large.\n"+
    "The maximum size for a multipart upload is 5TB.", bucketName)
  } else {
```

```
   log.Printf("Couldn't upload large object to %v:%v. Here's why: %v\n",
    bucketName, objectKey, err)
  }
 } else {
  err = s3.NewObjectExistsWaiter(basics.S3Client).Wait(
   ctx, &s3.HeadObjectInput{Bucket: aws.String(bucketName), Key:
 aws.String(objectKey)}, time.Minute)
  if err != nil {
   log.Printf("Failed attempt to wait for object %s to exist.\n", objectKey)
  }
 }

 return err
}
```

Example

Téléchargez un objet volumineux en utilisant un gestionnaire de téléchargement pour obtenir les données en plusieurs parties et les télécharger simultanément.

```
// DownloadLargeObject uses a download manager to download an object from a bucket.
// The download manager gets the data in parts and writes them to a buffer until all
 of
// the data has been downloaded.
func (basics BucketBasics) DownloadLargeObject(ctx context.Context, bucketName
 string, objectKey string) ([]byte, error) {
 var partMiBs int64 = 10
 downloader := manager.NewDownloader(basics.S3Client, func(d *manager.Downloader) {
  d.PartSize = partMiBs * 1024 * 1024
 })
 buffer := manager.NewWriteAtBuffer([]byte{})
 _, err := downloader.Download(ctx, buffer, &s3.GetObjectInput{
  Bucket: aws.String(bucketName),
  Key:    aws.String(objectKey),
 })
 if err != nil {
  log.Printf("Couldn't download large object from %v:%v. Here's why: %v\n",
   bucketName, objectKey, err)
 }
 return buffer.Bytes(), err
}
```

PHP

Cette rubrique explique comment utiliser la `Aws\S3\Model\MultipartUpload\UploadBuilder` classe de haut niveau de la AWS SDK pour PHP pour les téléchargements de fichiers en plusieurs parties. Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

L'exemple de code PHP ci-dessous permet de charger un fichier vers un compartiment Amazon S3. Il explique comment définir les paramètres de l'objet `MultipartUploader`.

```
 require 'vendor/autoload.php';

use Aws\Exception\MultipartUploadException;
use Aws\S3\MultipartUploader;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Prepare the upload parameters.
$uploader = new MultipartUploader($s3, '/path/to/large/file.zip', [
    'bucket' => $bucket,
    'key'    => $keyname
]);

// Perform the upload.
try {
    $result = $uploader->upload();
    echo "Upload complete: {$result['ObjectURL']}" . PHP_EOL;
} catch (MultipartUploadException $e) {
    echo $e->getMessage() . PHP_EOL;
}
```

Python

L'exemple suivant charge un objet à l'aide de l'API Python de haut niveau de chargements partitionnés (la classe `TransferManager`).

```
import sys
import threading

import boto3
from boto3.s3.transfer import TransferConfig


MB = 1024 * 1024
s3 = boto3.resource("s3")


class TransferCallback:
    """
    Handle callbacks from the transfer manager.

    The transfer manager periodically calls the __call__ method throughout
    the upload and download process so that it can take action, such as
    displaying progress to the user and collecting data about the transfer.
    """

    def __init__(self, target_size):
        self._target_size = target_size
        self._total_transferred = 0
        self._lock = threading.Lock()
        self.thread_info = {}

    def __call__(self, bytes_transferred):
        """
        The callback method that is called by the transfer manager.

        Display progress during file transfer and collect per-thread transfer
        data. This method can be called by multiple threads, so shared instance
        data is protected by a thread lock.
        """
        thread = threading.current_thread()
        with self._lock:
            self._total_transferred += bytes_transferred
            if thread.ident not in self.thread_info.keys():
                self.thread_info[thread.ident] = bytes_transferred
```

```
            else:
                self.thread_info[thread.ident] += bytes_transferred

            target = self._target_size * MB
            sys.stdout.write(
                f"\r{self._total_transferred} of {target} transferred "
                f"({(self._total_transferred / target) * 100:.2f}%)."
            )
            sys.stdout.flush()


def upload_with_default_configuration(
    local_file_path, bucket_name, object_key, file_size_mb
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, using the default
    configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_chunksize_and_meta(
    local_file_path, bucket_name, object_key, file_size_mb, metadata=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart chunk size and adding metadata to the Amazon S3 object.

    The multipart chunk size controls the size of the chunks of data that are
    sent in the request. A smaller chunk size typically results in the transfer
    manager using more threads for the upload.

    The metadata is a set of key-value pairs that are stored with the object
    in Amazon S3.
    """
    transfer_callback = TransferCallback(file_size_mb)

    config = TransferConfig(multipart_chunksize=1 * MB)
    extra_args = {"Metadata": metadata} if metadata else None
    s3.Bucket(bucket_name).upload_file(
```

```
        local_file_path,
        object_key,
        Config=config,
        ExtraArgs=extra_args,
        Callback=transfer_callback,
    )
    return transfer_callback.thread_info


def upload_with_high_threshold(local_file_path, bucket_name, object_key,
 file_size_mb):
    """
    Upload a file from a local folder to an Amazon S3 bucket, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard upload instead of
    a multipart upload.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).upload_file(
        local_file_path, object_key, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def upload_with_sse(
    local_file_path, bucket_name, object_key, file_size_mb, sse_key=None
):
    """
    Upload a file from a local folder to an Amazon S3 bucket, adding server-side
    encryption with customer-provided encryption keys to the object.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)
    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).upload_file(
```

```
        local_file_path, object_key, ExtraArgs=extra_args,
 Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_default_configuration(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using the
    default configuration.
    """
    transfer_callback = TransferCallback(file_size_mb)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_single_thread(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, using a
    single thread.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(use_threads=False)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_high_threshold(
    bucket_name, object_key, download_file_path, file_size_mb
):
    """
    Download a file from an Amazon S3 bucket to a local folder, setting a
    multipart threshold larger than the size of the file.

    Setting a multipart threshold larger than the size of the file results
    in the transfer manager sending the file as a standard download instead
```

```
    of a multipart download.
    """
    transfer_callback = TransferCallback(file_size_mb)
    config = TransferConfig(multipart_threshold=file_size_mb * 2 * MB)
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, Config=config, Callback=transfer_callback
    )
    return transfer_callback.thread_info


def download_with_sse(
    bucket_name, object_key, download_file_path, file_size_mb, sse_key
):
    """
    Download a file from an Amazon S3 bucket to a local folder, adding a
    customer-provided encryption key to the request.

    When this kind of encryption is specified, Amazon S3 encrypts the object
    at rest and allows downloads only when the expected encryption key is
    provided in the download request.
    """
    transfer_callback = TransferCallback(file_size_mb)

    if sse_key:
        extra_args = {"SSECustomerAlgorithm": "AES256", "SSECustomerKey": sse_key}
    else:
        extra_args = None
    s3.Bucket(bucket_name).Object(object_key).download_file(
        download_file_path, ExtraArgs=extra_args, Callback=transfer_callback
    )
    return transfer_callback.thread_info
```

Utilisation de AWS SDKs (API de bas niveau)

Le AWS SDK présente une API de bas niveau qui ressemble beaucoup à l'API REST d'Amazon S3 pour les téléchargements partitionnés (voir. Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3 Utilisez l'API de bas niveau lorsque vous devez suspendre et reprendre les téléchargements partitionnés, faire varier la taille des parties pendant le téléchargement ou si vous ne connaissez pas la taille des données de téléchargement à l'avance. Lorsque vous n'avez pas ces exigences, utilisez l'API de haut niveau (voirUtilisation de AWS SDKs (API de haut niveau)).

Java

L'exemple suivant montre comment utiliser les classes Java de bas niveau pour charger un fichier. Il exécute les étapes suivantes :

- Initie un chargement partitionné à l'aide de la méthode `AmazonS3Client.initiateMultipartUpload()` et transmet un objet `InitiateMultipartUploadRequest`.
- Enregistre l'ID de chargement renvoyé par la méthode `AmazonS3Client.initiateMultipartUpload()`. Vous devez fournir cet ID de chargement pour chaque opération suivante de chargement partitionné.
- Charge les parties de l'objet. Pour chaque partie, appelez la méthode `AmazonS3Client.uploadPart()`. Vous fournissez les informations de chargement de partie à l'aide d'un objet `UploadPartRequest`.
- Pour chaque partie, enregistre le ETag résultat de la réponse de la `AmazonS3Client.uploadPart()` méthode dans une liste. Vous utilisez les ETag valeurs pour terminer le téléchargement partitionné.
- Appelle la méthode `AmazonS3Client.completeMultipartUpload()` pour terminer le chargement partitionné.

Example

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.io.IOException;
import java.util.ArrayList;
import java.util.List;
```

```
public class LowLevelMultipartUpload {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String filePath = "*** Path to file to upload ***";

        File file = new File(filePath);
        long contentLength = file.length();
        long partSize = 5 * 1024 * 1024; // Set part size to 5 MB.

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Create a list of ETag objects. You retrieve ETags for each object
 part
            // uploaded,
            // then, after each individual part has been uploaded, pass the list of
 ETags to
            // the request to complete the upload.
            List<PartETag> partETags = new ArrayList<PartETag>();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
 InitiateMultipartUploadRequest(bucketName, keyName);
            InitiateMultipartUploadResult initResponse =
 s3Client.initiateMultipartUpload(initRequest);

            // Upload the file parts.
            long filePosition = 0;
            for (int i = 1; filePosition < contentLength; i++) {
                // Because the last part could be less than 5 MB, adjust the part
 size as
                // needed.
                partSize = Math.min(partSize, (contentLength - filePosition));

                // Create the request to upload a part.
                UploadPartRequest uploadRequest = new UploadPartRequest()
                        .withBucketName(bucketName)
                        .withKey(keyName)
```

```
                        .withUploadId(initResponse.getUploadId())
                        .withPartNumber(i)
                        .withFileOffset(filePosition)
                        .withFile(file)
                        .withPartSize(partSize);

                // Upload the part and add the response's ETag to our list.
                UploadPartResult uploadResult = s3Client.uploadPart(uploadRequest);
                partETags.add(uploadResult.getPartETag());

                filePosition += partSize;
            }

            // Complete the multipart upload.
            CompleteMultipartUploadRequest compRequest = new
 CompleteMultipartUploadRequest(bucketName, keyName,
                    initResponse.getUploadId(), partETags);
            s3Client.completeMultipartUpload(compRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

L'exemple C# suivant montre comment utiliser l'API de téléchargement SDK pour .NET partitionné de bas niveau pour télécharger un fichier dans un compartiment S3. Pour plus d'informations sur les chargements partitionnés Amazon S3, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

> **Note**
>
> Lorsque vous utilisez l' SDK pour .NET API pour télécharger des objets volumineux, un délai d'attente peut se produire lors de l'écriture des données dans le flux de demandes. Vous pouvez définir un délai explicite en utilisant `UploadPartRequest`.

L'exemple de code C# suivant charge un fichier dans un compartiment S3 grâce à l'API de chargement partitionné de bas niveau. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.Runtime;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadFileMPULowLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        private const string keyName = "*** provide a name for the uploaded object
 ***";
        private const string filePath = "*** provide the full path name of the file
 to upload ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Uploading an object");
            UploadObjectAsync().Wait();
        }
```

```
        private static async Task UploadObjectAsync()
        {
            // Create list to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = bucketName,
                Key = keyName
            };

            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // Upload parts.
            long contentLength = new FileInfo(filePath).Length;
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                Console.WriteLine("Uploading parts");

                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                        {
                            BucketName = bucketName,
                            Key = keyName,
                            UploadId = initResponse.UploadId,
                            PartNumber = i,
                            PartSize = partSize,
                            FilePosition = filePosition,
                            FilePath = filePath
                        };

                    // Track upload progress.
                    uploadRequest.StreamTransferProgress +=
                        new
EventHandler<StreamTransferProgressArgs>(UploadPartProgressEventCallback);
```

```
                    // Upload a part and add the response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

                    filePosition += partSize;
                }

                // Setup to complete the upload.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                    {
                        BucketName = bucketName,
                        Key = keyName,
                        UploadId = initResponse.UploadId
                     };
                completeRequest.AddPartETags(uploadResponses);

                // Complete the upload.
                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown: { 0}",
exception.Message);

                // Abort the upload.
                AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    UploadId = initResponse.UploadId
                };
               await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
        }
        public static void UploadPartProgressEventCallback(object sender,
StreamTransferProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
```

```
    }
}
```

PHP

Cette rubrique explique comment utiliser la `uploadPart` méthode de bas niveau de la version 3 de AWS SDK pour PHP pour télécharger un fichier en plusieurs parties. Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

L'exemple PHP suivant charge un fichier dans un compartiment Amazon S3 grâce au chargement partitionné de l'API PHP de bas niveau.

```
 require 'vendor/autoload.php';

use Aws\S3\Exception\S3Exception;
use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$filename = '*** Path to and Name of the File to Upload ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

$result = $s3->createMultipartUpload([
    'Bucket'       => $bucket,
    'Key'          => $keyname,
    'StorageClass' => 'REDUCED_REDUNDANCY',
    'Metadata'     => [
        'param1' => 'value 1',
        'param2' => 'value 2',
        'param3' => 'value 3'
    ]
]);
$uploadId = $result['UploadId'];

// Upload the file in parts.
try {
    $file = fopen($filename, 'r');
    $partNumber = 1;
    while (!feof($file)) {
```

```
        $result = $s3->uploadPart([
            'Bucket'     => $bucket,
            'Key'        => $keyname,
            'UploadId'   => $uploadId,
            'PartNumber' => $partNumber,
            'Body'       => fread($file, 5 * 1024 * 1024),
        ]);
        $parts['Parts'][$partNumber] = [
            'PartNumber' => $partNumber,
            'ETag' => $result['ETag'],
        ];
        $partNumber++;

        echo "Uploading part $partNumber of $filename." . PHP_EOL;
    }
    fclose($file);
} catch (S3Exception $e) {
    $result = $s3->abortMultipartUpload([
        'Bucket'   => $bucket,
        'Key'      => $keyname,
        'UploadId' => $uploadId
    ]);

    echo "Upload of $filename failed." . PHP_EOL;
}

// Complete the multipart upload.
$result = $s3->completeMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
    'MultipartUpload'    => $parts,
]);
$url = $result['Location'];

echo "Uploaded $filename to $url." . PHP_EOL;
```

À l'aide du AWS SDK pour Ruby

La AWS SDK pour Ruby version 3 prend en charge les téléchargements partitionnés sur Amazon S3 de deux manières. Pour la première option, vous pouvez utiliser des chargements de fichiers gérés. Pour plus d'informations, consultez Uploading Files to Amazon S3 dans le Blog des développeurs

AWS . Les chargements de fichiers gérés constituent la méthode recommandée pour charger des fichiers dans un compartiment. Ces chargements offrent les avantages suivants :

- Ils gèrent les chargements partitionnés pour les objets de plus de 15 Mo.
- Ils ouvrent correctement les fichiers en mode binaire pour éviter les problèmes d'encodage.
- Ils utilisent plusieurs threads pour le chargement des parties d'objets volumineux en parallèle.

Vous pouvez également utiliser directement les opérations suivantes du client de chargement partitionné :

- create_multipart_upload – Lance un chargement partitionné et renvoie un ID de chargement.
- upload_part – Charge une partie d'un chargement partitionné.
- upload_part_copy – Charge une partie en copiant les données d'un objet existant comme source de données.
- complete_multipart_upload – Termine un chargement partitionné en assemblant des parties chargées précédemment.
- abort_multipart_upload – Arrête un chargement partitionné.

Chargement d'un répertoire à l'aide de la classe TransferUtility .

Vous pouvez utiliser la classe `TransferUtility` pour charger un répertoire entier. Par défaut, l'API charge uniquement les fichiers à la racine du répertoire spécifié. Toutefois, vous pouvez spécifier de charger les fichiers de manière récursive dans tous les sous-répertoires.

Indiquez des expressions de filtre pour sélectionner des fichiers dans le répertoire spécifié selon des critères de filtrage. Par exemple, pour ne charger que les fichiers PDF d'un répertoire, spécifiez l'expression de filtre `"*.pdf"`.

Quand vous chargez des données depuis un répertoire, vous ne spécifiez pas les noms de clé pour les objets résultants. Amazon S3 génère les noms de clé à l'aide du chemin du fichier d'origine. Par exemple, si vous avez un répertoire appelé `c:\myfolder` avec la structure suivante :

Example

```
C:\myfolder
      \a.txt
      \b.pdf
      \media\
```

```
            An.mp3
```

Lorsque vous chargez ce répertoire, Amazon S3 utilise les noms de clé suivants :

Example

```
a.txt
b.pdf
media/An.mp3
```

Example

L'exemple C# suivant charge un répertoire dans un compartiment Amazon S3. Il montre comment utiliser différentes surcharges `TransferUtility.UploadDirectory` pour charger le répertoire. Chaque appel de chargement successif remplace le chargement précédent. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.IO;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class UploadDirMPUHighLevelAPITest
    {
        private const string existingBucketName = "*** bucket name ***";
        private const string directoryPath = @"*** directory path ***";
        // The example uploads only .txt files.
        private const string wildCard = "*.txt";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion = RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            UploadDirAsync().Wait();
        }
```

```
        private static async Task UploadDirAsync()
        {
            try
            {
                var directoryTransferUtility =
                    new TransferUtility(s3Client);

                // 1. Upload a directory.
                await directoryTransferUtility.UploadDirectoryAsync(directoryPath,
                    existingBucketName);
                Console.WriteLine("Upload statement 1 completed");

                // 2. Upload only the .txt files from a directory
                //    and search recursively.
                await directoryTransferUtility.UploadDirectoryAsync(
                                                directoryPath,
                                                existingBucketName,
                                                wildCard,
                                                SearchOption.AllDirectories);
                Console.WriteLine("Upload statement 2 completed");

                // 3. The same as Step 2 and some optional configuration.
                //    Search recursively for .txt files to upload.
                var request = new TransferUtilityUploadDirectoryRequest
                {
                    BucketName = existingBucketName,
                    Directory = directoryPath,
                    SearchOption = SearchOption.AllDirectories,
                    SearchPattern = wildCard
                };

                await directoryTransferUtility.UploadDirectoryAsync(request);
                Console.WriteLine("Upload statement 3 completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an object",
e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
```

```
                    "Unknown encountered on server. Message:'{0}' when writing an
 object", e.Message);
                }
            }
        }
}
```

Liste des chargements partitionnés

Vous pouvez utiliser l' AWS CLI API REST ou AWS SDKs, pour récupérer une liste des téléchargements partitionnés en cours dans Amazon S3. Vous pouvez utiliser le chargement partitionné pour charger par programme un seul objet sur Amazon S3. Les chargements partitionnés déplacent un objet vers Amazon S3 en déplaçant des portions des données de cet objet à la fois. Pour en savoir plus sur le chargement partitionné, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Pour une end-to-end procédure de téléchargement d'un objet avec un téléchargement en plusieurs parties avec une somme de contrôle supplémentaire, voir. Didacticiel : chargement partitionné d'un objet et vérification de l'intégrité de ses données

La section suivante explique comment répertorier les téléchargements partitionnés en cours avec l' AWS Command Line Interface API REST Amazon S3 et. AWS SDKs

Répertorier les téléchargements partitionnés à l'aide du AWS CLI

Les sections suivantes AWS Command Line Interface décrivent les opérations de listage des téléchargements partitionnés.

- list-parts- répertorie les parties chargées pour un chargement partitionné spécifique.
- list-multipart-uploads-liste les téléchargements partitionnés en cours.

Liste des chargements partitionnés à l'aide de l'API REST

Les sections suivantes de la Référence de l'API Amazon Simple Storage Service décrivent l'API REST pour la liste des chargements partitionnés.

- ListParts-liste les parties téléchargées pour un téléchargement en plusieurs parties spécifique.
- ListMultipartUploads-liste les téléchargements partitionnés en cours.

Répertorier les téléchargements partitionnés à l'aide du AWS SDK (API de bas niveau)

Java

Les tâches suivantes vous guident dans l'utilisation des classes Java de bas niveau pour répertorier tous les chargements partitionnés en cours sur un compartiment.

Processus d'élaboration de la liste des chargements partitionnés via l'API de bas niveau

1	Créez une instance de la classe `ListMultipartUploadsRequest` et précisez le nom du compartiment.
2	Exécutez la méthode `AmazonS3Client.listMultipartUploads`. Cette méthode renvoie une instance de la classe `MultipartUploadListing`, qui vous fournit des informations sur les chargements partitionnés en cours.

L'exemple de code Java suivant présente les tâches précédentes.

Example

```
ListMultipartUploadsRequest allMultpartUploadsRequest =
     new ListMultipartUploadsRequest(existingBucketName);
MultipartUploadListing multipartUploadListing =
     s3Client.listMultipartUploads(allMultpartUploadsRequest);
```

.NET

Pour afficher tous les chargements partitionnés en cours vers un compartiment spécifique, utilisez la classe `ListMultipartUploadsRequest` de l'API de chargement partitionné de bas niveau du kit SDK pour .NET . La méthode `AmazonS3Client.ListMultipartUploads` retourne une instance de la classe `ListMultipartUploadsResponse` qui fournit des informations sur les chargements partitionnés en cours.

Un chargement partitionné en cours est un chargement partitionné qui a été lancé à l'aide d'une demande de lancement de chargement partitionné, mais qui n'a pas encore été terminé ou arrêté. Pour en savoir plus sur les chargements partitionnés Amazon S3, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

L'exemple C# suivant montre comment utiliser le pour SDK pour .NET répertorier tous les téléchargements partitionnés en cours sur un bucket. Pour plus d'informations sur la configuration

et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
ListMultipartUploadsRequest request = new ListMultipartUploadsRequest
{
  BucketName = bucketName // Bucket receiving the uploads.
};

ListMultipartUploadsResponse response = await
 AmazonS3Client.ListMultipartUploadsAsync(request);
```

PHP

Cette rubrique explique comment utiliser les classes d'API de bas niveau de la version 3 de AWS SDK pour PHP pour répertorier tous les téléchargements partitionnés en cours sur un bucket. Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

L'exemple PHP suivant montre comment répertorier tous les chargements partitionnés en cours sur un compartiment.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Retrieve a list of the current multipart uploads.
$result = $s3->listMultipartUploads([
    'Bucket' => $bucket
]);

// Write the list of uploads to the page.
print_r($result->toArray());
```

Suivi d'un téléchargement en plusieurs parties à l'aide du AWS SDKs

Vous pouvez suivre la progression du chargement d'un objet vers Amazon S3 à l'aide d'une interface d'écoute. L'API de chargement partitionné de haut niveau fournit une interface d'écoute appelée `ProgressListener`. Les événements de progression ont lieu de manière périodique et informent l'écouteur que des octets ont été transférés. Pour en savoir plus sur le chargement partitionné, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Pour une end-to-end procédure de téléchargement d'un objet avec un téléchargement en plusieurs parties avec une somme de contrôle supplémentaire, voir. Didacticiel : chargement partitionné d'un objet et vérification de l'intégrité de ses données

La section suivante explique comment suivre un téléchargement partitionné avec le AWS SDKs.

Java

Example

```
TransferManager tm = new TransferManager(new ProfileCredentialsProvider());

PutObjectRequest request = new PutObjectRequest(
    existingBucketName, keyName, new File(filePath));

// Subscribe to the event and provide event handler.
request.setProgressListener(new ProgressListener() {
   public void progressChanged(ProgressEvent event) {
    System.out.println("Transferred bytes: " +
      event.getBytesTransfered());
            }
});
```

Example

L'exemple de code Java suivant charge un fichier et utilise le `ProgressListener` pour suivre la progression du chargement. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, consultez Getting Started dans le guide du AWS SDK pour Java développeur.

```
import java.io.File;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.event.ProgressEvent;
```

```
import com.amazonaws.event.ProgressListener;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.Upload;

public class TrackMPUProgressUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide bucket name ***";
        String keyName            = "*** Provide object key ***";
        String filePath           = "*** file to upload ***";

        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());


        // For more advanced uploads, you can create a request object
        // and supply additional request parameters (ex: progress listeners,
        // canned ACLs, etc.)
        PutObjectRequest request = new PutObjectRequest(
          existingBucketName, keyName, new File(filePath));

        // You can ask the upload for its progress, or you can
        // add a ProgressListener to your request to receive notifications
        // when bytes are transferred.
        request.setGeneralProgressListener(new ProgressListener() {
   @Override
   public void progressChanged(ProgressEvent progressEvent) {
    System.out.println("Transferred bytes: " +
      progressEvent.getBytesTransferred());
   }
  });

        // TransferManager processes all transfers asynchronously,
        // so this call will return immediately.
        Upload upload = tm.upload(request);

        try {
         // You can block and wait for the upload to finish
         upload.waitForCompletion();
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload aborted.");
         amazonClientException.printStackTrace();
        }
    }
```

```
}
```

.NET

L'exemple C# suivant charge un fichier dans un compartiment S3 à l'aide de la classe `TransferUtility` et suit la progression du chargement. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class TrackMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide the bucket name ***";
        private const string keyName = "*** provide the name for the uploaded object
 ***";
        private const string filePath = " *** provide the full path name of the file
 to upload **";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;


        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            TrackMPUAsync().Wait();
        }

        private static async Task TrackMPUAsync()
        {
            try
            {
                var fileTransferUtility = new TransferUtility(s3Client);

                // Use TransferUtilityUploadRequest to configure options.
```

```
                // In this example we subscribe to an event.
                var uploadRequest =
                    new TransferUtilityUploadRequest
                    {
                        BucketName = bucketName,
                        FilePath = filePath,
                        Key = keyName
                    };

                uploadRequest.UploadProgressEvent +=
                    new EventHandler<UploadProgressArgs>
                        (uploadRequest_UploadPartProgressEvent);

                await fileTransferUtility.UploadAsync(uploadRequest);
                Console.WriteLine("Upload completed");
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }

        static void uploadRequest_UploadPartProgressEvent(object sender,
 UploadProgressArgs e)
        {
            // Process event.
            Console.WriteLine("{0}/{1}", e.TransferredBytes, e.TotalBytes);
        }
    }
}
```

Interruption d'un chargement partitionné

Après avoir lancé un chargement partitionné, vous commencez à charger les parties. Amazon S3 stocke ces parties et ne crée l'objet qu'une fois que vous avez chargé toutes les parties et envoyé une demande de finalisation du chargement partitionné. Dès réception de la demande de fin de

chargement partitionné, Amazon S3 assemble les parties et crée un objet. Si vous n'envoyez pas correctement la demande de finalisation du chargement partitionné, S3 n'assemble pas les différentes parties et ne crée aucun objet. Si vous ne souhaitez pas finaliser un chargement partitionné après avoir chargé différentes parties, vous devez abandonner le chargement partitionné.

Vous êtes facturé pour tout le stockage associé aux parties chargées. Il est recommandé de toujours finaliser le chargement partitionné ou d'arrêter le chargement partitionné pour supprimer les parties chargées. Pour de plus amples informations sur la tarification, consultez Chargement partitionné et tarification.

Vous pouvez également arrêter un chargement partitionné incomplet à l'aide d'une configuration de cycle de vie de compartiment. Pour de plus amples informations, veuillez consulter Configuration d'une configuration de cycle de vie de compartiment pour supprimer les chargements partitionnés incomplets.

La section suivante explique comment arrêter un chargement partitionné en cours dans Amazon S3 à l'aide de l' AWS Command Line Interface API REST ou. AWS SDKs

À l'aide du AWS CLI

Pour plus d'informations sur l'utilisation du AWS CLI pour arrêter un téléchargement partitionné, consultez abort-multipart-uploadla référence des AWS CLI commandes.

Utilisation de l'API REST

Pour plus d'informations sur l'utilisation de l'API REST pour arrêter un téléchargement AbortMultipartUploaden plusieurs parties, consultez le manuel Amazon Simple Storage Service API Reference.

Utilisation de AWS SDKs (API de haut niveau)

Java

La classe `TransferManager` fournit la méthode `abortMultipartUploads` pour arrêter les chargements partitionnés en cours. Un chargement est considéré comme étant en cours dès que vous le lancez et jusqu'à ce qu'il soit terminé ou arrêté. Vous fournissez une valeur `Date`, et cette API arrête tous les chargements partitionnés dans ce compartiment qui avaient été lancés avant la `Date` spécifiée et qui sont toujours en cours.

Les tâches suivantes vous guident tout au long de l'utilisation des classes Java de haut niveau pour arrêter les chargements partitionnés.

Processus d'arrêt des chargements partitionnés grâce à l'API de haut niveau

1	Créez une instance de la classe `TransferManager` .
2	Exécutez la méthode `TransferManager.abortMultipartUploads` en indiquant le nom du compartiment et une valeur `Date`.

Le code Java suivant arrête tous les chargements partitionnés en cours initiés dans un compartiment spécifique, il y a plus d'une semaine. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, consultez Getting Started dans le guide du AWS SDK pour Java développeur.

```
import java.util.Date;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3.transfer.TransferManager;

public class AbortMPUUsingHighLevelAPI {

    public static void main(String[] args) throws Exception {
        String existingBucketName = "*** Provide existing bucket name ***";

        TransferManager tm = new TransferManager(new ProfileCredentialsProvider());


        int sevenDays = 1000 * 60 * 60 * 24 * 7;
  Date oneWeekAgo = new Date(System.currentTimeMillis() - sevenDays);

        try {
         tm.abortMultipartUploads(existingBucketName, oneWeekAgo);
        } catch (AmazonClientException amazonClientException) {
         System.out.println("Unable to upload file, upload was aborted.");
         amazonClientException.printStackTrace();
        }
    }
}
```

> **Note**
>
> Vous pouvez également arrêter un chargement partitionné spécifique. Pour plus d'informations, consultez Utilisation de AWS SDKs (API de bas niveau).

.NET

L'exemple C# suivant arrête tous les chargements partitionnés en cours initiés sur un compartiment spécifique il y a plus d'une semaine. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Transfer;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class AbortMPUUsingHighLevelAPITest
    {
        private const string bucketName = "*** provide bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            AbortMPUAsync().Wait();
        }

        private static async Task AbortMPUAsync()
        {
            try
            {
                var transferUtility = new TransferUtility(s3Client);
```

```
                // Abort all in-progress uploads initiated before the specified
 date.
                await transferUtility.AbortMultipartUploadsAsync(
                    bucketName, DateTime.Now.AddDays(-7));
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

> **Note**
>
> Vous pouvez également arrêter un chargement partitionné spécifique. Pour de plus amples informations, veuillez consulter Utilisation de AWS SDKs (API de bas niveau).

Utilisation de AWS SDKs (API de bas niveau)

Vous pouvez arrêter un chargement partitionné en cours en appelant la méthode `AmazonS3.abortMultipartUpload`. Cette méthode supprime toutes les parties qui ont été chargées dans Amazon S3 et libère les ressources. Vous devez fournir l'ID de chargement, le nom du compartiment et le nom de la clé. L'exemple de code Java suivant illustre comment arrêter un chargement partitionné en cours.

Pour arrêter un chargement partitionné, vous fournissez l'ID de chargement, ainsi que les noms de compartiment et de clé utilisés dans le chargement. Après avoir arrêté un chargement partitionné, vous ne pouvez pas utiliser l'ID de chargement pour charger les parties supplémentaires. Pour en savoir plus sur les chargements partitionnés Amazon S3, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Java

L'exemple de code Java suivant arrête un chargement partitionné en cours.

Example

```
InitiateMultipartUploadRequest initRequest =
    new InitiateMultipartUploadRequest(existingBucketName, keyName);
InitiateMultipartUploadResult initResponse =
               s3Client.initiateMultipartUpload(initRequest);

AmazonS3 s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
s3Client.abortMultipartUpload(new AbortMultipartUploadRequest(
            existingBucketName, keyName, initResponse.getUploadId()));
```

> **Note**
>
> Au lieu d'un chargement partitionné spécifique, vous pouvez arrêter tous vos chargements partitionnés démarrés avant un moment spécifique et qui sont toujours en cours. Cette opération de nettoyage est utile pour arrêter les anciens chargements partitionnés que vous avez initiés mais que vous n'avez pas terminés ou arrêtés. Pour plus d'informations, consultez Utilisation de AWS SDKs (API de haut niveau).

.NET

L'exemple C# suivant montre comment arrêter un chargement partitionné. Pour obtenir un exemple C# complet incluant le code suivant, consultez Utilisation de AWS SDKs (API de bas niveau).

```
AbortMultipartUploadRequest abortMPURequest = new AbortMultipartUploadRequest
{
    BucketName = existingBucketName,
    Key = keyName,
    UploadId = initResponse.UploadId
};
await AmazonS3Client.AbortMultipartUploadAsync(abortMPURequest);
```

Vous pouvez aussi annuler tous les chargements partitionnés en cours démarrés avant un moment spécifique. Cette opération de nettoyage est utile pour abandonner les chargements

partitionnés que vous n'avez pas terminés ou interrompus. Pour plus d'informations, consultez Utilisation de AWS SDKs (API de haut niveau).

PHP

Cet exemple illustre comment utiliser une classe de la version 3 du kit AWS SDK pour PHP pour interrompre un chargement partitionné en cours. Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2. L'exemple de la méthode `abortMultipartUpload()`.

Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';
$uploadId = '*** Upload ID of upload to Abort ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Abort the multipart upload.
$s3->abortMultipartUpload([
    'Bucket'   => $bucket,
    'Key'      => $keyname,
    'UploadId' => $uploadId,
]);
```

Copie d'un objet à l'aide du chargement partitionné

Le chargement partitionné vous permet de copier des objets en plusieurs parties. Les exemples de cette section vous montrent comment copier des objets supérieurs à 5 Go grâce à l'API de chargement partitionné. Pour plus d'informations sur les chargements partitionnés, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Vous pouvez copier les objets inférieurs à 5 Go en une seule opération sans avoir à utiliser l'API de chargement partitionné. Vous pouvez copier des objets de moins de 5 Go à l' AWS Management

Console aide de l'API REST, ou AWS SDKs. AWS CLI Pour de plus amples informations, veuillez consulter Copie, déplacement et changement de nom des objets.

Pour une end-to-end procédure de téléchargement d'un objet avec un téléchargement en plusieurs parties avec une somme de contrôle supplémentaire, voir. Didacticiel : chargement partitionné d'un objet et vérification de l'intégrité de ses données

La section suivante explique comment copier un objet avec un téléchargement partitionné à l'aide de l'API REST ou AWS SDKs.

Utilisation de l'API REST

Les sections suivantes de la Référence de l'API Amazon Simple Storage Service décrivent l'API REST pour le chargement partitionné. Pour copier un objet existant, utilisez l'API de chargement d'une partie (Copy) et spécifiez l'objet source en ajoutant l'en-tête `x-amz-copy-source` dans votre demande.

- Lancement du chargement partitionné
- Chargement d'une partie
- Chargement d'une partie (Copy)
- Achèvement du chargement partitionné
- Interruption du chargement partitionné
- Liste des parties
- Liste des chargements partitionnés

Vous pouvez les utiliser APIs pour effectuer vos propres requêtes REST, ou vous pouvez utiliser l'une des solutions SDKs que nous proposons. Pour plus d'informations sur l'utilisation du téléchargement partitionné avec AWS CLI le. À l'aide du AWS CLI Pour plus d'informations sur le SDKs, consultezAWS Support du SDK pour le téléchargement en plusieurs parties.

À l'aide du AWS SDKs

Pour copier un objet à l'aide de l'API de bas niveau, procédez comme suit :

- Lancez un chargement partitionné en appelant la méthode `AmazonS3Client.initiateMultipartUpload()`.

- Enregistrez l'ID de chargement de l'objet de la réponse renvoyé par la méthode `AmazonS3Client.initiateMultipartUpload()`. Vous devez fournir cet ID de chargement pour chaque opération de chargement de partie.
- Copiez toutes les parties. Pour chaque partie que vous devez copier, créez une nouvelle instance de la classe `CopyPartRequest`. Fournissez les informations sur la partie, notamment les noms des compartiments source et de destination, les clés d'objet source et de destination, l'ID de chargement, les emplacement des premier et dernier octets de la partie, ainsi que le numéro de la partie.
- Enregistrez les réponses des appels de méthode `AmazonS3Client.copyPart()`. Chaque réponse inclut la valeur `ETag` et le numéro de partie de la partie chargée. Vous avez besoin de ces informations pour terminer le chargement partitionné.
- Appelez la méthode `AmazonS3Client.completeMultipartUpload()` pour terminer l'opération de copie.

Java

Example

L'exemple suivant montre comment utiliser l'API Java de bas niveau Amazon S3 pour effectuer une copie en plusieurs parties. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;
import java.util.List;

public class LowLevelMultipartCopy {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String sourceBucketName = "*** Source bucket name ***";
```

```
        String sourceObjectKey = "*** Source object key ***";
        String destBucketName = "*** Target bucket name ***";
        String destObjectKey = "*** Target object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
InitiateMultipartUploadRequest(destBucketName,
                    destObjectKey);
            InitiateMultipartUploadResult initResult =
s3Client.initiateMultipartUpload(initRequest);

            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest(sourceBucketName, sourceObjectKey);
            ObjectMetadata metadataResult =
s3Client.getObjectMetadata(metadataRequest);
            long objectSize = metadataResult.getContentLength();

            // Copy the object using 5 MB parts.
            long partSize = 5 * 1024 * 1024;
            long bytePosition = 0;
            int partNum = 1;
            List<CopyPartResult> copyResponses = new ArrayList<CopyPartResult>();
            while (bytePosition < objectSize) {
                // The last part might be smaller than partSize, so check to make
sure
                // that lastByte isn't beyond the end of the object.
                long lastByte = Math.min(bytePosition + partSize - 1, objectSize -
1);

                // Copy this part.
                CopyPartRequest copyRequest = new CopyPartRequest()
                        .withSourceBucketName(sourceBucketName)
                        .withSourceKey(sourceObjectKey)
                        .withDestinationBucketName(destBucketName)
                        .withDestinationKey(destObjectKey)
                        .withUploadId(initResult.getUploadId())
                        .withFirstByte(bytePosition)
```

```
                        .withLastByte(lastByte)
                        .withPartNumber(partNum++);
                copyResponses.add(s3Client.copyPart(copyRequest));
                bytePosition += partSize;
            }

            // Complete the upload request to concatenate all uploaded parts and
 make the
            // copied object available.
            CompleteMultipartUploadRequest completeRequest = new
 CompleteMultipartUploadRequest(
                    destBucketName,
                    destObjectKey,
                    initResult.getUploadId(),
                    getETags(copyResponses));
            s3Client.completeMultipartUpload(completeRequest);
            System.out.println("Multipart copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    // This is a helper function to construct a list of ETags.
    private static List<PartETag> getETags(List<CopyPartResult> responses) {
        List<PartETag> etags = new ArrayList<PartETag>();
        for (CopyPartResult response : responses) {
            etags.add(new PartETag(response.getPartNumber(), response.getETag()));
        }
        return etags;
    }
}
```

.NET

L'exemple C# suivant montre comment utiliser le SDK pour .NET pour copier un objet Amazon S3 d'une taille supérieure à 5 Go d'un emplacement source à un autre, par exemple d'un

compartiment à un autre. Pour copier des objets dont la taille est inférieure à 5 Go, utilisez la procédure de copie en une seule opération décrite dans À l'aide du AWS SDKs. Pour en savoir plus sur les chargements partitionnés Amazon S3, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Cet exemple montre comment copier un objet Amazon S3 d'une taille supérieure à 5 Go d'un compartiment S3 vers un autre à l'aide de l'API de téléchargement SDK pour .NET partitionné.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectUsingMPUapiTest
    {
        private const string sourceBucket = "*** provide the name of the bucket with
 source object ***";
        private const string targetBucket = "*** provide the name of the bucket to
 copy the object to ***";
        private const string sourceObjectKey = "*** provide the name of object to
 copy ***";
        private const string targetObjectKey = "*** provide the name of the object
 copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            MPUCopyObjectAsync().Wait();
        }
        private static async Task MPUCopyObjectAsync()
        {
            // Create a list to store the upload part responses.
            List<UploadPartResponse> uploadResponses = new
 List<UploadPartResponse>();
```

```
            List<CopyPartResponse> copyResponses = new List<CopyPartResponse>();

            // Setup information required to initiate the multipart upload.
            InitiateMultipartUploadRequest initiateRequest =
                new InitiateMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey
                };

            // Initiate the upload.
            InitiateMultipartUploadResponse initResponse =
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // Save the upload ID.
            String uploadId = initResponse.UploadId;

            try
            {
                // Get the size of the object.
                GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest
                {
                    BucketName = sourceBucket,
                    Key = sourceObjectKey
                };

                GetObjectMetadataResponse metadataResponse =
                    await s3Client.GetObjectMetadataAsync(metadataRequest);
                long objectSize = metadataResponse.ContentLength; // Length in
bytes.

                // Copy the parts.
                long partSize = 5 * (long)Math.Pow(2, 20); // Part size is 5 MB.

                long bytePosition = 0;
                for (int i = 1; bytePosition < objectSize; i++)
                {
                    CopyPartRequest copyRequest = new CopyPartRequest
                    {
                        DestinationBucket = targetBucket,
                        DestinationKey = targetObjectKey,
                        SourceBucket = sourceBucket,
                        SourceKey = sourceObjectKey,
```

```
                        UploadId = uploadId,
                        FirstByte = bytePosition,
                        LastByte = bytePosition + partSize - 1 >= objectSize ?
 objectSize - 1 : bytePosition + partSize - 1,
                        PartNumber = i
                    };

                    copyResponses.Add(await s3Client.CopyPartAsync(copyRequest));

                    bytePosition += partSize;
                }

                // Set up to complete the copy.
                CompleteMultipartUploadRequest completeRequest =
                new CompleteMultipartUploadRequest
                {
                    BucketName = targetBucket,
                    Key = targetObjectKey,
                    UploadId = initResponse.UploadId
                };
                completeRequest.AddPartETags(copyResponses);

                // Complete the copy.
                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

Didacticiel : chargement partitionné d'un objet et vérification de l'intégrité de ses données

Le chargement partitionné vous permet de charger un seul objet en tant qu'ensemble de parties. Chaque partie est une portion contiguë des données de l'objet. Vous pouvez charger ces parties d'objet indépendamment et dans n'importe quel ordre. Si le transfert d'une partie échoue, vous pouvez la retransférer sans affecter les autres. Une fois toutes les parties de l'objet chargées, Amazon S3 les assemble et crée l'objet. En général, lorsque l'objet atteint la taille de 100 Mo, vous devez préférer les chargements partitionnés au chargement d'objet en une seule opération. Pour en savoir plus sur les chargements partitionnés, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3. Pour obtenir les limites liées aux chargements partitionnés, consultez Limites de la fonction de chargement partitionné Amazon S3.

Vous pouvez utiliser des sommes de contrôle pour vérifier que les ressources ne sont pas altérées lors de la copie. L'exécution d'une somme de contrôle consiste à utiliser un algorithme pour itérer séquentiellement chaque octet d'un fichier. Amazon S3 propose plusieurs options de somme de contrôle pour vérifier l'intégrité des données. Nous vous recommandons d'effectuer ces contrôles d'intégrité en tant que bonne pratique de durabilité et pour confirmer que chaque octet est transféré sans modification. Amazon S3 prend également en charge les algorithmes suivants : SHA-1, SHA-256 et C. CRC32 CRC32 Amazon S3 utilise un ou plusieurs de ces algorithmes pour calculer la valeur d'une somme de contrôle supplémentaire et la stocker dans les métadonnées de l'objet. Pour en savoir plus sur le total de contrôle, consultez Vérification de l'intégrité des objets dans Amazon S3.

Objectif

Dans ce didacticiel, vous allez apprendre à charger un objet sur Amazon S3 à l'aide d'un téléchargement en plusieurs parties et d'une somme de contrôle SHA-256 supplémentaire via l'interface de ligne de AWS commande (CLI).AWS Vous apprendrez également à vérifier l'intégrité des données de l'objet en calculant le MD5 hachage et la somme de contrôle SHA-256 de l'objet chargé.

Rubriques

- Prérequis
- Étape 1 : création d'un gros fichier
- Étape 2 : division du fichier en plusieurs fichiers
- Étape 3 : création du chargement partitionné avec une somme de contrôle supplémentaire
- Étape 4 : chargement des différentes parties du chargement partitionné

- Étape 5 : affichage de la liste de toutes les parties du chargement partitionné
- Étape 6 : finalisation du chargement partitionné
- Étape 7 : vérification du chargement de l'objet est dans votre compartiment
- Étape 8 : vérifier l'intégrité de l'objet à l'aide d'une somme MD5 de contrôle
- Étape 9 : vérification de l'intégrité de l'objet à l'aide d'une somme de contrôle supplémentaire
- Étape 10 : nettoyage de vos ressources

Prérequis

- Avant de commencer ce didacticiel, vérifiez que vous avez accès à un compartiment Amazon S3 dans lequel vous pouvez charger un objet. Pour de plus amples informations, veuillez consulter Création d'un bucket à usage général.
- La AWS CLI doit être installée et configurée. Pour installer l'interface de ligne de commande AWS , consultez Installation ou mise à jour de la dernière version de l' AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface .
- Vous pouvez également exécuter des commandes AWS CLI depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? et Mise en route AWS CloudShell dans le guide de AWS CloudShell l'utilisateur.

Étape 1 : création d'un gros fichier

Si vous avez déjà un fichier prêt à être chargé, vous pouvez l'utiliser pour ce didacticiel. Dans le cas contraire, créez un fichier de 15 Mo en procédant comme suit. Pour obtenir les limites liées aux chargements partitionnés, consultez Limites de la fonction de chargement partitionné Amazon S3.

Pour créer un gros fichier

Utilisez l'une des commandes suivantes pour créer le fichier, selon le système d'exploitation que vous utilisez.

Linux ou macOS

Pour créer un fichier de 15 Mo, ouvrez votre terminal local et exécutez la commande suivante :

```
dd if=/dev/urandom of=census-data.bin bs=1M count=15
```

Cette commande crée un fichier nommé `census-data.bin` rempli d'octets aléatoires, d'une taille de 15 Mo.

Windows

Pour créer un fichier de 15 Mo, ouvrez votre terminal local et exécutez la commande suivante :

```
fsutil file createnew census-data.bin 15728640
```

Cette commande crée un fichier nommé `census-data.bin` avec une taille de 15 Mo de données arbitraires (15 728 640 octets).

Étape 2 : division du fichier en plusieurs fichiers

Pour effectuer le chargement partitionné, vous devez diviser le gros fichier en parties de plus petite taille. Vous pourrez ensuite charger ces parties de plus petite taille en utilisant le processus de chargement partitionné. Cette étape montre comment diviser le gros fichier créé à l'étape 1 en plusieurs parties de plus petite taille. L'exemple suivant utilise un fichier de 15 Mo nommé `census-data.bin`.

Pour diviser un gros fichier en plusieurs parties

Linux ou macOS

Pour diviser le gros fichier en parties de 5 Mo, utilisez la commande `split`. Ouvrez le terminal et exécutez ce qui suit :

```
split -b 5M -d census-data.bin census-part
```

Cette commande divise `census-data.bin` en parties de 5 Mo nommées `census-part**`, où `**` est un suffixe numérique commençant par `00`.

Windows

Pour scinder le gros fichier, utilisez PowerShell. Ouvrez PowerShell et exécutez le script suivant :

```
$inputFile = "census-data.bin"
$outputFilePrefix = "census-part"
$chunkSize = 5MB

$fs = [System.IO.File]::OpenRead($inputFile)
```

```
$buffer = New-Object byte[] $chunkSize
$fileNumber = 0

while ($fs.Position -lt $fs.Length) {
$bytesRead = $fs.Read($buffer, 0, $chunkSize)
$outputFile = "{0}{1:D2}" -f $outputFilePrefix, $fileNumber
$fileStream = [System.IO.File]::Create($outputFile)
$fileStream.Write($buffer, 0, $bytesRead)
$fileStream.Close()
$fileNumber++
}

$fs.Close()
```

Ce PowerShell script lit le gros fichier par blocs de 5 Mo et écrit chaque bloc dans un nouveau fichier avec un suffixe numérique.

Après avoir exécuté la commande appropriée, vous devriez voir les différentes parties dans le répertoire dans lequel vous l'avez exécutée. Chaque partie a un suffixe correspondant à son numéro de partie, par exemple :

```
census-part00 census-part01 census-part02
```

Étape 3 : création du chargement partitionné avec une somme de contrôle supplémentaire

Pour pouvoir lancer le processus de chargement partitionné, vous devez créer la demande de chargement partitionné. Cette étape consiste à lancer le chargement partitionné et à spécifier une somme de contrôle supplémentaire pour l'intégrité des données. L'exemple suivant utilise la somme de contrôle SHA-256. Si vous souhaitez fournir des métadonnées qui décrivent l'objet en cours de chargement, vous devez le faire dans la demande de lancement du chargement partitionné.

> **Note**
>
> Dans cette étape et dans les étapes suivantes, ce didacticiel utilise l'algorithme supplémentaire SHA-256. Vous pouvez éventuellement utiliser une autre somme de contrôle supplémentaire pour ces étapes, telle que CRC32 CRC32 C ou SHA-1. Si vous choisissez un algorithme différent, vous devrez l'utiliser tout au long des étapes de ce didacticiel.

Pour lancer le chargement partitionné

Sur le terminal, utilisez la commande `create-multipart-upload` suivante afin de lancer un chargement partitionné pour votre compartiment. Remplacez *amzn-s3-demo-bucket1* par le nom de votre compartiment. Remplacez également `census_data_file` par le nom de fichier que vous avez choisi. Ce nom de fichier deviendra la clé d'objet une fois le chargement terminé.

```
aws s3api create-multipart-upload --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --checksum-algorithm sha256
```

Si la demande aboutit, vous obtenez une sortie JSON semblable à la suivante :

```
{
    "ServerSideEncryption": "AES256",
    "ChecksumAlgorithm": "SHA256",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "UploadId":
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqyb8m3
}
```

> **Note**
>
> Lorsque vous envoyez une demande pour lancer un chargement partitionné, Amazon S3 renvoie une réponse avec un ID de chargement, qui est un identifiant unique pour le chargement partitionné. Vous devez inclure cet ID de chargement dès que vous chargez les parties, listez les parties, terminez un chargement ou arrêtez un chargement. Vous devrez utiliser les valeurs `UploadId`, `Key` et `Bucket` pour les étapes ultérieures. Veillez donc à les enregistrer.
>
> Si vous utilisez un chargement partitionné avec des sommes de contrôle supplémentaires, les numéros des différentes parties doivent être consécutifs. Dans le cas contraire, la demande `complete-multipart-upload` pourra générer une erreur HTTP `500 Internal Server Error`.

Étape 4 : chargement des différentes parties du chargement partitionné

Au cours de cette étape, vous chargerez les parties du chargement partitionné dans le compartiment S3. Utilisez la commande `upload-part` pour charger chaque partie individuellement. Ce processus

nécessite de spécifier l'ID de chargement, le numéro des parties et le fichier à charger pour chaque partie.

Pour charger les différentes parties de l'objet

1. Lorsque vous chargez une partie, outre l'ID de chargement, vous devez spécifier un numéro de partie à l'aide de l'argument `--part-number`. Vous pouvez choisir n'importe quel numéro de partie compris entre 1 et 10 000. Un numéro de partie identifie de manière unique une partie et sa place dans l'objet que vous chargez. Le numéro de partie que vous choisissez doit obligatoirement constituer une séquence consécutive (par exemple, 1, 2 ou 3). Si vous chargez une nouvelle partie avec le même numéro qu'une partie précédemment chargée, cette dernière est remplacée.
2. Utilisez la commande `upload-part` pour charger chaque partie du chargement partitionné. L'`--upload-id` est le même que dans la sortie créée par la commande `create-multipart-upload` à l'étape 3. Pour charger la première partie de vos données, utilisez la commande suivante :

   ```
   aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
    'census_data_file' --part-number 1 --body census-part00 --upload-id
    "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
    --checksum-algorithm SHA256
   ```

   À la fin de chaque commande `upload-part`, vous devriez voir une sortie semblable à l'exemple suivant :

   ```
   {
       "ServerSideEncryption": "AES256",
       "ETag": "\"e611693805e812ef37f96c9937605e69\"",
       "ChecksumSHA256": "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0="
   }
   ```

3. Pour les parties suivantes, incrémentez leur numéro en conséquence :

   ```
   aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
   part-number <part-number> --body <file-path> --upload-id "<your-upload-id>" --
   checksum-algorithm SHA256
   ```

Par exemple, utilisez la commande suivante pour charger la deuxième partie :

```
aws s3api upload-part --bucket amzn-s3-demo-bucket1 --key
 'census_data_file' --part-number 2 --body census-part01 --upload-id
 "cNV6KCSNANFZapz1LUGPC5XwUVi1n6yUoIeSP138sNOKPeMhpKQRrbT9k0ePmgoOTCj9K83T4e2Gb5hQvNoNpCKqy
 --checksum-algorithm SHA256
```

Amazon S3 renvoie un tag d'entité (ETag) et des sommes de contrôle supplémentaires pour chaque partie téléchargée sous forme d'en-tête dans la réponse.

4. Continuez à utiliser la commande `upload-part` jusqu'à ce que vous ayez chargé toutes les parties de l'objet.

Étape 5 : affichage de la liste de toutes les parties du chargement partitionné

Pour finaliser le chargement partitionné, vous aurez besoin d'une liste de toutes les parties qui ont été chargées pour ce chargement partitionné spécifique. Le résultat de la `list-parts` commande fournit des informations telles que le nom du compartiment, la clé, l'ID de téléchargement, le numéro de pièce ETag, des sommes de contrôle supplémentaires, etc. Il est utile d'enregistrer cette sortie dans un fichier afin de pouvoir l'utiliser à l'étape suivante lorsque vous finaliserez le processus de chargement partitionné. Vous pouvez créer un fichier de sortie JSON appelé `parts.json` en utilisant la méthode suivante.

Pour créer un fichier répertoriant toutes les parties

1. Pour générer un fichier JSON contenant les détails de toutes les parties chargées, utilisez la commande `list-parts` suivante. Remplacez ***amzn-s3-demo-bucket1*** par le nom réel de votre compartiment et **<your-upload-id>** par l'ID de chargement que vous avez reçu à l'étape 3. Pour plus d'informations sur la commande `list-parts`, consultez list-parts dans le Guide de l'utilisateur AWS Command Line Interface .

   ```
   aws s3api list-parts --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --
   upload-id <your-upload-id> --query '{Parts: Parts[*].{PartNumber: PartNumber, ETag:
    ETag, ChecksumSHA256: ChecksumSHA256}}' --output json > parts.json
   ```

   Un nouveau fichier appelé `parts.json` est généré. Ce fichier contient les informations, au format JSON, de toutes les parties que vous avez chargées. Le `parts.json` fichier contient des informations essentielles pour chaque partie de votre téléchargement partitionné, telles que les

numéros de pièce et les ETag valeurs correspondantes, qui sont nécessaires pour terminer le processus de téléchargement partitionné.

2. Ouvrez `parts.json` à l'aide de n'importe quel éditeur de texte ou via le terminal. Voici l'exemple de sortie :

```
{
    "Parts": [
        {
            "PartNumber": 1,
            "ETag": "\"3c3097f89e2a2fece47ac54b243c9d97\"",
            "ChecksumSHA256": "fTPVHfyNHdv5VkR4S3EewdyioXECv7JBxN+d4FXYYTw="
        },
        {
            "PartNumber": 2,
            "ETag": "\"03c71cc160261b20ab74f6d2c476b450\"",
            "ChecksumSHA256": "VDWTa8enjOvULBAO3W2a6C+5/7ZnNjrnLApa1QVc3FE="
        },
        {
            "PartNumber": 3,
            "ETag": "\"81ae0937404429a97967dffa7eb4affb\"",
            "ChecksumSHA256": "cVVkXehUlzcwrBrXgPIM+EKQXPUvWist8mlUTCs4bg8="
        }
    ]
}
```

Étape 6 : finalisation du chargement partitionné

Après le chargement et l'affichage de toutes les parties du chargement partitionné, la dernière étape consiste à finaliser le chargement partitionné. Cette étape fusionne toutes les parties chargées en un seul objet dans votre compartiment S3.

> **Note**
>
> Vous pouvez calculer la somme de contrôle de l'objet avant d'appeler `complete-multipart-upload` en incluant `--checksum-sha256` dans votre demande. Si les sommes ne correspondent pas, Amazon S3 ne répondra pas à la demande. Pour plus

d'informations, consultez complete-multipart-upload dans le Guide de l'utilisateur AWS Command Line Interface .

Pour finaliser le chargement partitionné

Pour finaliser le chargement partitionné, utilisez la commande `complete-multipart-upload`. Cette commande nécessite le fichier `parts.json` créé à l'étape 5, le nom de votre compartiment et l'ID de chargement. Remplacez **<*amzn-s3-demo-bucket1*>** par le nom de votre compartiment et **<your-upload-id>** par l'ID de chargement de `parts.json`.

```
aws s3api complete-multipart-upload --multipart-upload file://parts.json --bucket amzn-s3-demo-bucket1 --key 'census_data_file' --upload-id <your-upload-id>
```

Voici l'exemple de sortie :

```
{
    "ServerSideEncryption": "AES256",
    "Location": "https://amzn-s3-demo-bucket1.s3.us-east-2.amazonaws.com/census_data_file",
    "Bucket": "amzn-s3-demo-bucket1",
    "Key": "census_data_file",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3"
}
```

> **Note**
>
> Ne supprimez pas encore les fichiers de chaque partie chargée. Vous en aurez besoin pour pouvoir effectuer des sommes de contrôles correspondantes afin de vérifier l'intégrité de l'objet fusionné.

Étape 7 : vérification du chargement de l'objet est dans votre compartiment

Une fois le chargement partitionné finalisé, vous pouvez vérifier que l'objet a bien été chargé dans votre compartiment S3. Pour répertorier les objets de votre compartiment et confirmer la présence du fichier qui vient d'être chargé, utilisez la commande `list-objects-v2`.

Pour répertorier l'objet chargé

Pour répertorier les objets de votre compartiment, utilisez la commande `list-objects-v2`. Remplacez ***amzn-s3-demo-bucket1*** par le nom de votre compartiment :

```
aws s3api list-objects-v2 --bucket amzn-s3-demo-bucket1
```

Cette commande renvoie une liste des objets qui se trouvent dans votre compartiment. Recherchez le fichier que vous avez chargé (par exemple, `census_data_file`) dans la liste des objets.

Pour plus d'informations, consultez la section Exemples correspondant à la commande `list-objects-v2` dans le Guide de l'utilisateur AWS Command Line Interface .

Étape 8 : vérifier l'intégrité de l'objet à l'aide d'une somme MD5 de contrôle

Lorsque vous chargez un objet, vous pouvez spécifier un algorithme de somme de contrôle à utiliser par Amazon S3. Par défaut, Amazon S3 stocke le MD5 condensé d'octets sous la forme de celui de l'objet ETag. Pour les chargements partitionnés, ETag il ne s'agit pas de la somme de contrôle pour l'objet entier, mais plutôt d'un composite des sommes de contrôle pour chaque partie individuelle.

Pour vérifier l'intégrité d'un objet à l'aide d'une somme MD5 de contrôle

1. Pour récupérer ETag l'objet téléchargé, effectuez une `head-object` requête :

   ```
   aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file
   ```

   Voici l'exemple de sortie :

   ```
   {
       "AcceptRanges": "bytes",
       "LastModified": "2024-07-26T19:04:13+00:00",
       "ContentLength": 16106127360,
       "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
       "ContentType": "binary/octet-stream",
       "ServerSideEncryption": "AES256",
       "Metadata": {}
   }
   ```

« -3 » ETag est ajouté à la fin. Cela indique que l'objet a été chargé en trois parties à l'aide du chargement partitionné.

2. Ensuite, calculez la MD5 somme de contrôle de chaque pièce à l'aide de la `md5sum` commande. Veillez à fournir le chemin d'accès correct vers les fichiers partiels :

```
md5sum census-part*
```

Voici l'exemple de sortie :

```
e611693805e812ef37f96c9937605e69 census-part00
63d2d5da159178785bfd6b6a5c635854 census-part01
95b87c7db852451bb38b3b44a4e6d310 census-part02
```

3. Pour cette étape, combinez manuellement les MD5 hachages en une seule chaîne. Exécutez ensuite la commande suivante pour convertir la chaîne en binaire et calculer la MD5 somme de contrôle de la valeur binaire :

```
echo
 "e611693805e812ef37f96c9937605e6963d2d5da159178785bfd6b6a5c63585495b87c7db852451bb38b3b44a
 | xxd -r -p | md5sum
```

Voici l'exemple de sortie :

```
f453c6dccca969c457efdf9b1361e291 -
```

Cette valeur de hachage doit correspondre à la valeur de hachage de la ETag valeur d'origine de l'étape 1, qui valide l'intégrité de l'objet. `census_data_file`

Lorsque vous demandez à Amazon S3 d'utiliser des totaux de contrôle supplémentaires, Amazon S3 calcule la valeur du total de contrôle pour chaque partie et stocke les valeurs. Pour récupérer les valeurs de somme de contrôle de chaque partie des chargements partitionnés qui sont toujours en cours, vous pouvez utiliser `list-parts`.

Pour plus d'informations sur le fonctionnement des sommes de contrôle avec les objets d'un chargement partitionné, consultez Vérification de l'intégrité des objets dans Amazon S3.

Étape 9 : vérification de l'intégrité de l'objet à l'aide d'une somme de contrôle supplémentaire

Dans cette étape, ce didacticiel utilise SHA-256 comme somme de contrôle supplémentaire pour valider l'intégrité de l'objet. Si vous avez opté pour une somme de contrôle supplémentaire différente, utilisez cette valeur.

Pour vérifier l'intégrité des objets avec SHA256

1. Exécutez la commande suivante dans le terminal, y compris l'argument `--checksum-mode enabled`, pour afficher la valeur `ChecksumSHA256` de l'objet :

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key census_data_file --
checksum-mode enabled
```

   Voici l'exemple de sortie :

```
{
    "AcceptRanges": "bytes",
    "LastModified": "2024-07-26T19:04:13+00:00",
    "ContentLength": 16106127360,
    "ChecksumSHA256": "aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=-3",
    "ETag": "\"f453c6dccca969c457efdf9b1361e291-3\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {}
}
```

2. Utilisez les commandes suivantes pour décoder les valeurs `ChecksumSHA256` des différentes parties en base64 et les enregistrer dans un fichier binaire appelé `outfile`. Ces valeurs se trouvent dans le fichier `parts.json`. Remplacez les exemples de chaînes base64 par vos valeurs `ChecksumSHA256` réelles.

```
echo "QLl8R4i4+SaJlrl8ZIcutc5TbZtwt2NwB8lTXkd3GH0=" | base64 --decode >> outfile
echo "xCdgs1K5Bm4jWETYw/CmGYr+m6O2DcGfpckx5NVokvE=" | base64 --decode >> outfile
echo "f5wsfsa5bB+yXuwzqG1Bst91uYneqGD3CCidpb54mAo=" | base64 --decode >> outfile
```

3. Exécutez la commande suivante pour calculer la SHA256 somme de contrôle de `outfile` :

```
sha256sum outfile
```

Voici l'exemple de sortie :

```
688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9 outfile
```

À l'étape suivante, convertissez la valeur de hachage en valeur binaire. Cette valeur binaire doit correspondre à la valeur `ChecksumSHA256` de l'étape 1.

4. Convertissez la SHA256 somme de contrôle de l'étape 3 en binaire, puis encodez-la en base64 pour vérifier qu'elle correspond à la `ChecksumSHA256` valeur de l'étape 1 :

```
echo "688f04a24b42768b6353c06ae3a0eb3c2c50086b8670f221279d67a16b3a86f9" | xxd -r -p
 | base64
```

Voici l'exemple de sortie :

```
aI8EoktCdotjU8Bq46DrPCxQCGuGcPIhJ51noWs6hvk=
```

Cette sortie devrait confirmer que la sortie base64 correspond à la valeur `ChecksumSHA256` de la sortie de la commande `head-object`. Si la sortie correspond à la valeur de la somme de contrôle, l'objet est valide.

> **Important**
>
> - Lorsque vous demandez à Amazon S3 d'utiliser des sommes de contrôle supplémentaires, Amazon S3 calcule les valeurs de sommes de contrôle pour chaque partie et les stocke.
> - Pour récupérer les valeurs de somme de contrôle de chaque partie des chargements partitionnés qui sont toujours en cours, vous pouvez utiliser la commande `list-parts`.

Étape 10 : nettoyage de vos ressources

Si vous souhaitez nettoyer les fichiers créés dans ce didacticiel, appliquez la méthode suivante. Pour obtenir des instructions sur la suppression des fichiers chargés dans votre compartiment S3, consultez Suppression d'objets Amazon S3.

Supprimez les fichiers locaux créés à l'étape 1 :

Pour supprimer les fichiers que vous avez créés pour le chargement partitionné, exécutez la commande suivante à partir de votre répertoire de travail :

```
rm census-data.bin census-part* outfile parts.json
```

Limites de la fonction de chargement partitionné Amazon S3

Le chargement partitionné vous permet de charger un seul objet en tant qu'ensemble de parties. Chaque partie est une portion contiguë des données de l'objet. Une fois toutes les parties de l'objet chargées, Amazon S3 les assemble et crée l'objet. En général, lorsque l'objet atteint la taille de 100 Mo, vous devez préférer les chargements partitionnés au chargement d'objet en une seule opération. Pour en savoir plus sur les chargements partitionnés, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Le tableau suivant fournit les principales spécifications du chargement partitionné. Elles incluent notamment la taille maximale de l'objet, le nombre maximal de parties, la taille maximale de chaque partie, etc. Il n'existe pas de limite de taille minimale pour la dernière partie de votre chargement partitionné.

Élément	Spécification
Taille maximum de l'objet	5 TiO
Nombre maximum de parties par chargement	10 000
Numéros de partie	1 à 10 000 (inclus)
Taille de partie	5 Mio à 5 GiO. Il n'existe pas de limite de taille minimale pour la dernière partie de votre chargement partitionné.
Nombre maximum de parties renvoyées pour une demande de liste des parties	1 000
Nombre maximum de chargements partitionnés renvoyés dans une	1 000

Élément	Spécification
demande de liste de chargements partitionnés	

Ajout de conditions préalables aux opérations S3 avec des demandes conditionnelles

Vous pouvez utiliser des demandes conditionnelles pour ajouter des conditions préalables à vos opérations S3. Pour utiliser des demandes conditionnelles, vous devez ajouter un en-tête supplémentaire à votre opération d'API Amazon S3. Cet en-tête spécifie une condition qui, si elle n'est pas remplie, entraînera l'échec de l'opération S3.

Les lectures conditionnelles sont prises en charge pour les demandes `GET`, `HEAD` et `COPY`. Vous pouvez ajouter des conditions préalables pour renvoyer ou copier un objet en fonction de sa balise Entity (ETag) ou de sa date de dernière modification. Cela permet de limiter une opération S3 aux objets mis à jour depuis une date spécifiée. Vous pouvez également limiter une opération S3 à une opération spécifique ETag. Cela permet de garantir que vous ne renvoyez ou ne copiez qu'une version d'objet spécifique. Pour en savoir plus sur les métadonnées d'objet, consultez Utilisation des métadonnées d'objet.

Les écritures conditionnelles permettent de garantir qu'aucun objet ne porte le même nom de clé dans votre compartiment pendant les opérations `PUT`. Cela empêche l'écrasement d'objets existants portant des noms de clé identiques. De même, vous pouvez utiliser les écritures conditionnelles pour vérifier si l'objet ETag est inchangé avant de le mettre à jour. Cela permet d'éviter les écrasements involontaires d'un objet sans connaître l'état de son contenu. Vous pouvez utiliser des écritures conditionnelles pour les demandes PutObject ou CompleteMultipartUpload. Pour en savoir plus sur les noms de clé, consultez Attribution d'un nom aux objets Amazon S3.

Les lectures ou écritures conditionnelles n'entraînent pas de frais supplémentaires. Vous ne payez que les tarifs existants pour les demandes applicables, y compris celles ayant échoué. Pour en savoir plus sur les fonctions et la tarification d'Amazon S3, consultez Tarification Amazon S3.

Rubriques

- Comment récupérer ou copier des objets en fonction des métadonnées avec des lectures conditionnelles
- Comment empêcher le remplacement d'objets par des écritures conditionnelles

Comment récupérer ou copier des objets en fonction des métadonnées avec des lectures conditionnelles

Avec les lectures conditionnelles, vous pouvez inclure un en-tête supplémentaire à votre demande de lecture afin d'ajouter des conditions préalables à votre opération S3. Si ces conditions préalables ne sont pas remplies, la demande de lecture échouera.

Vous pouvez utiliser des lectures conditionnelles au niveau des demandes `GET`, `HEAD` ou `COPY` pour ne renvoyer un objet qu'en fonction de ses métadonnées.

Lorsque vous chargez un objet, Amazon S3 crée des métadonnées contrôlées par le système qui ne peuvent être modifiées que par S3. Les balises d'entité (ETags) et Last-Modified sont des exemples de métadonnées contrôlées par le système. Un objet ETag est une chaîne représentant une version spécifique d'un objet. La date de dernière modification fait partie des métadonnées représentant la date de création ou la date de la dernière modification de l'objet, la date la plus récente étant retenue.

Avec les lectures conditionnelles, vous pouvez renvoyer un objet en fonction de sa date de dernière modification ETag ou de sa date de dernière modification. Vous pouvez spécifier une ETag valeur avec votre demande et renvoyer l'objet uniquement si la ETag valeur correspond. Cela vous permet de ne renvoyer ou ne copier qu'une version spécifique d'un objet. Vous pouvez spécifier une valeur de dernière modification dans votre demande de lecture et ne renvoyer que les objets modifiés depuis une date que vous avez indiquée.

Soutenu APIs

Le APIs support S3 suivant utilise des lectures conditionnelles :

- GetObject
- HeadObject
- CopyObject

Vous pouvez utiliser les en-têtes suivants pour renvoyer un objet en fonction de la balise d'entité (ETag) ou de la date de dernière modification. Pour plus d'informations sur les métadonnées d'objets telles que ETags et Last-Modified, consultez. the section called "Métadonnées d'objet définies par le système"

GetObject

- `If-Match`— Renvoie l'objet uniquement s'il ETag correspond à celui fourni.
- `If-Modified-Since` : renvoie l'objet uniquement s'il a été modifié depuis l'heure spécifiée.
- `If-None-Match`— Renvoie l'objet uniquement s'il ETag ne correspond pas à celui fourni.
- `If-Unmodified-Since` : renvoie l'objet uniquement s'il n'a pas été modifié depuis l'heure spécifiée.

Pour plus d'informations sur ces en-têtes, les erreurs renvoyées et l'ordre dans lequel S3 gère plusieurs en-têtes conditionnels dans une seule demande, consultez GetObject dans la Référence d'API Amazon Simple Storage Service.

HeadObject

- `If-Match`— Renvoie l'objet uniquement s'il ETag correspond à celui fourni.
- `If-Modified-Since` : renvoie l'objet uniquement s'il a été modifié depuis l'heure spécifiée.
- `If-None-Match`— Renvoie l'objet uniquement s'il ETag ne correspond pas à celui fourni.
- `If-Unmodified-Since` : renvoie l'objet uniquement s'il n'a pas été modifié depuis l'heure spécifiée.

Pour plus d'informations sur ces en-têtes, les erreurs renvoyées et l'ordre dans lequel S3 gère plusieurs en-têtes conditionnels dans une seule demande, consultez HeadObject dans la Référence d'API Amazon Simple Storage Service.

CopyObject

- `x-amz-copy-source-if-match`— Copie l'objet source uniquement s'il ETag correspond à celui fourni.
- `x-amz-copy-source-if-modified-since` : copie l'objet source uniquement s'il a été modifié depuis l'heure spécifiée.
- `x-amz-copy-source-if-none-match`— Copie l'objet source uniquement s'il ETag ne correspond pas à celui fourni.
- `x-amz-copy-source-if-unmodified-since` : copie l'objet source uniquement s'il n'a pas été modifié depuis l'heure spécifiée.

Pour plus d'informations sur ces en-têtes, les erreurs renvoyées et l'ordre dans lequel S3 gère plusieurs en-têtes conditionnels dans une seule demande, consultez CopyObject dans la Référence d'API Amazon Simple Storage Service.

Comment empêcher le remplacement d'objets par des écritures conditionnelles

Avec les écritures conditionnelles, vous pouvez ajouter un en-tête supplémentaire à vos demandes `WRITE` afin de spécifier les conditions préalables à une opération Amazon S3. Pour écrire des objets de manière conditionnelle, ajoutez l'en-tête HTTP `If-None-Match` ou `If-Match`.

L'en-tête `If-None-Match` empêche le remplacement de données existantes en validant qu'aucun objet portant le même nom de clé ne se trouve déjà dans votre compartiment.

Vous pouvez également ajouter l'`If-Match`en-tête pour vérifier la balise d'entité (ETag) d'un objet avant d'écrire un objet. Avec cet en-tête, Amazon S3 compare la ETag valeur fournie avec la ETag valeur de l'objet dans S3. Si les ETag valeurs ne correspondent pas, l'opération échoue.

Les propriétaires de compartiments peuvent utiliser des politiques de compartiment pour appliquer des écritures conditionnelles aux objets chargés. Pour de plus amples informations, veuillez consulter the section called "Application d'écritures conditionnelles".

> **Note**
>
> Pour utiliser des écritures conditionnelles, vous devez effectuer les demandes via HTTPS (TLS) ou utiliser AWS Signature Version 4 afin de signer la demande.

Rubriques

- Comment empêcher le remplacement d'objets en fonction des noms de clé
- Comment empêcher les remplacements si l'objet a changé
- Comportement des écritures conditionnelles
- Scénarios d'écritures conditionnelles
- Application d'écritures conditionnelles sur des compartiments Amazon S3

Comment empêcher le remplacement d'objets en fonction des noms de clé

Avant de créer un objet, vous pouvez utiliser l'en-tête conditionnel HTTP `If-None-Match` pour vérifier si cet objet existe déjà dans le compartiment spécifié en fonction de son nom de clé. Lorsque vous chargez un objet sur Amazon S3, vous spécifiez le nom de la clé, qui est un identifiant unique, sensible à la casse, d'un objet dans un compartiment. Sans l'en-tête HTTP `If-None-Match`, si vous chargez un objet avec un nom de clé identique dans un compartiment pour lequel la gestion des versions est suspendue ou n'est pas activée, l'objet sera remplacé. Dans un compartiment pour lequel la gestion des versions est activée, l'objet le plus récemment chargé devient la version actuelle de l'objet. Les écritures conditionnelles avec l'en-tête HTTP `If-None-Match` vérifient l'existence d'un objet pendant l'opération `WRITE`. Si un nom de clé identique est trouvé dans le compartiment, l'opération échoue. Pour en savoir plus sur l'utilisation des noms de clé, consultez the section called "Attribution d'un nom aux objets".

Pour effectuer des écritures conditionnelles avec l'en-tête HTTP `If-None-Match`, vous devez avoir l'autorisation `s3:PutObject`. Cela permet à l'appelant de vérifier la présence d'objets dans le compartiment. L'en-tête `If-None-Match` s'attend à recevoir la valeur * (astérisque).

Vous pouvez utiliser l'`If-None-Match`en-tête avec les éléments suivants APIs :

- PutObject
- CompleteMultipartUpload

À l'aide du AWS CLI

L'exemple de commande `put-object` suivant tente d'effectuer une écriture conditionnelle pour un objet portant le nom de clé `dir-1/my_images.tar.bz2`.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-none-match "*"
```

Pour plus d'informations, consultez put-object dans la Référence des commandes de l'AWS CLI .

Pour plus d'informations sur le AWS CLI, voir Qu'est-ce que le AWS Command Line Interface ? dans le guide de AWS Command Line Interface l'utilisateur.

Comment empêcher les remplacements si l'objet a changé

Un objet ETag est une chaîne unique à l'objet qui reflète une modification du contenu de l'objet. Vous pouvez utiliser l'`If-Match`en-tête pour comparer la ETag valeur d'un objet dans un compartiment

Amazon S3 avec celle que vous avez fournie pendant l'`WRITE`opération. Si les ETag valeurs ne correspondent pas, l'opération échoue. Pour plus d'informations sur ETags, voirthe section called "Utilisation du contenu MD5 et du ETag pour vérifier les objets téléchargés".

Pour effectuer des écritures conditionnelles avec un en-tête HTTP `If-Match`, vous devez disposer des autorisations `s3:PutObject` et `s3:GetObject`. Cela permet à l'appelant de vérifier ETag et de vérifier l'état des objets contenus dans le compartiment. L'`If-Match`en-tête attend la ETag valeur sous forme de chaîne.

Vous pouvez utiliser l'`If-Match`en-tête avec les éléments suivants APIs :

- PutObject
- CompleteMultipartUpload

À l'aide du AWS CLI

L'`put-object`exemple de commande suivant tente d'effectuer une écriture conditionnelle avec la ETag valeur fournie`6805f2cfc46c0f04559748bb039d69ae`.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key dir-1/my_images.tar.bz2 --body
 my_images.tar.bz2 --if-match "6805f2cfc46c0f04559748bb039d69ae"
```

Pour plus d'informations, consultez put-object dans la Référence des commandes de l'AWS CLI .

Pour plus d'informations sur le AWS CLI, voir Qu'est-ce que le AWS Command Line Interface ? dans le guide de AWS Command Line Interface l'utilisateur.

Comportement des écritures conditionnelles

Écritures conditionnelles avec l'en-tête **`If-None-Match`**

Les écritures conditionnelles avec l'en-tête `If-None-Match` sont évaluées par rapport aux objets existants dans un compartiment. S'il n'existe aucun objet portant le même nom de clé dans le compartiment, l'opération d'écriture réussit, ce qui entraîne une réponse `200 OK`. S'il existe un objet, l'opération d'écriture échoue, ce qui entraîne une réponse `412 Precondition Failed`.

Pour les compartiments pour lesquels la gestion des versions est activée, s'il n'existe aucune version d'objet portant le même nom, ou si la version actuelle de l'objet est un marqueur de suppression, l'opération d'écriture réussit. Dans le cas contraire, l'opération d'écriture échoue avec une réponse `412 Precondition Failed`.

Si plusieurs écritures conditionnelles ont lieu pour le même nom d'objet, la première opération d'écriture à se terminer aboutit. Amazon S3 abandonne alors les écritures suivantes avec une réponse `412 Precondition Failed`.

Vous pouvez également recevoir une réponse `409 Conflict` en cas de demandes simultanées si une demande de suppression d'un objet aboutit avant la fin d'une opération d'écriture conditionnelle sur cet objet. Lorsque vous utilisez des écritures conditionnelles avec `PutObject`, les chargements peuvent faire l'objet d'une nouvelle tentative après réception d'une erreur `409 Conflict`. Lors de l'utilisation de `CompleteMultipartUpload`, le chargement partitionné complet doit être relancé avec `CreateMultipartUpload` pour charger à nouveau l'objet après réception d'une erreur `409 Conflict`.

Écritures conditionnelles avec l'en-tête **`If-Match`**

L'en-tête `If-Match` est évalué par rapport aux objets existants dans un compartiment. S'il existe un objet portant le même nom de clé et correspondant ETag, l'opération d'écriture réussit, ce qui entraîne une `200 OK` réponse. Si ce ETag n'est pas le cas, l'opération d'écriture échoue avec une `412 Precondition Failed` réponse.

Vous pouvez également recevoir une réponse `409 Conflict` en cas de demandes simultanées.

Vous recevrez une réponse `404 Not Found` si une demande de suppression simultanée d'un objet aboutit avant la fin d'une opération d'écriture conditionnelle sur cet objet, car la clé de l'objet n'existe plus. Lorsque vous recevez une réponse `404 Not Found`, vous devez charger à nouveau l'objet.

S'il n'existe aucune version d'objet portant le même nom, ou si la version actuelle de l'objet est un marqueur de suppression, l'opération échoue avec une erreur `404 Not Found`.

Scénarios d'écritures conditionnelles

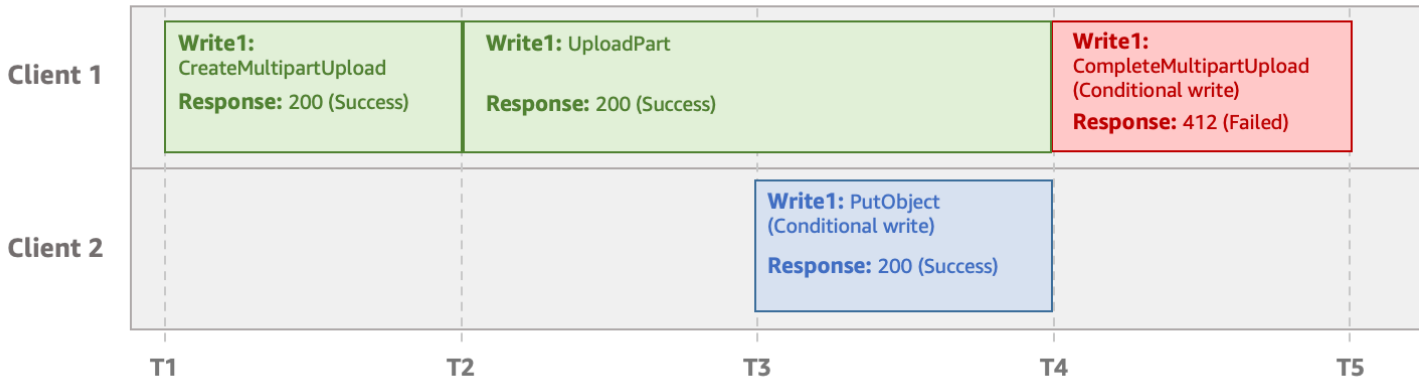
Examinez les scénarios suivants dans lesquels deux clients exécutent des opérations sur le même compartiment.

Écritures conditionnelles lors des chargements partitionnés

Les écritures conditionnelles ne prennent pas en compte les demandes de chargement partitionné en cours, car il ne s'agit pas encore d'objets entièrement écrits. Prenons l'exemple suivant où le client 1 charge un objet à l'aide du chargement partitionné. Pendant le chargement partitionné, le client 2

est en mesure d'écrire avec succès ce même objet grâce à l'opération d'écriture conditionnelle. Par la suite, lorsque le client 1 essaie de finaliser le chargement partitionné à l'aide d'une écriture conditionnelle, le chargement échoue.

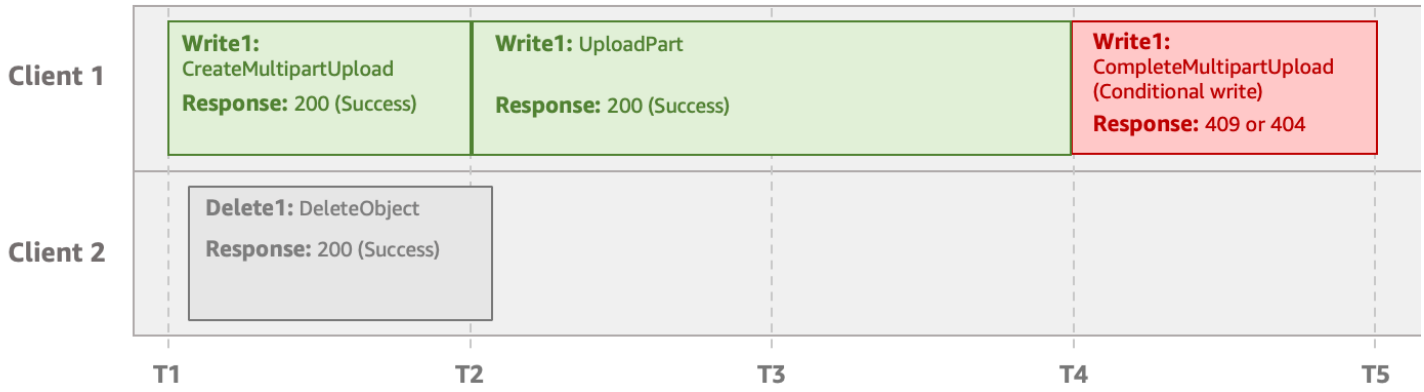
> **Note**
>
> Ce scénario entraîne une réponse `412 Precondition Failed` à la fois pour les en-têtes en-têtes `If-None-Match` et `If-Match`.



Suppressions simultanées lors de chargements partitionnés

Si une demande de suppression aboutit avant qu'une demande d'écriture conditionnelle ne se termine, Amazon S3 renvoie une réponse `409 Conflict` ou `404 Not Found` pour l'opération d'écriture. Cela est dû au fait que la demande de suppression initiée précédemment a priorité sur l'opération d'écriture conditionnelle. Dans ce cas, vous devrez lancer un nouveau chargement partitionné.

> **Note**
>
> Ce scénario génère une réponse `409 Conflict` pour un en-tête `If-None-Match` et une réponse `404 Not Found` pour un en-tête `If-Match`.



> **Note**
>
> Pour réduire vos coûts de stockage, nous vous recommandons de configurer une règle du cycle de vie pour supprimer les chargements partitionnés incomplets après un certain nombre de jours à l'aide de l'action `AbortIncompleteMultipartUpload`. Pour plus d'informations sur la création d'une règle de cycle de vie pour supprimer les chargements partitionnés incomplets, consultez Configuration d'une politique de cycle de vie de compartiment pour abandonner les chargements multiparties incomplets.

Application d'écritures conditionnelles sur des compartiments Amazon S3

Avec des politiques de compartiments Amazon S3, vous pouvez appliquer des écritures conditionnelles pour les chargements d'objets dans vos compartiments à usage général.

Une politique de compartiment est une politique basée sur les ressources que vous pouvez utiliser pour accorder des autorisations d'accès à votre compartiment Amazon S3 et aux objets qu'il contient. Seul le propriétaire du compartiment peut associer une politique à un compartiment. Pour plus d'informations sur les stratégies de compartiment, consultez the section called "Politiques de compartiment".

Vous pouvez utiliser les clés de condition `s3:if-match` ou `Condition` comme élément `s3:if-none-match` ou bloc `Condition` facultatif pour spécifier des conditions lorsqu'une politique est appliquée. Pour les téléchargements partitionnés, vous devez spécifier la clé de `s3:ObjectCreationOperation` condition pour exempter les `UploadPartCopy` opérations`CreateMultipartUpload`, et`UploadPart`, car celles-ci APIs n'acceptent pas les en-

têtes conditionnels. Pour plus d'informations sur l'utilisation de conditions dans les politiques de compartiment, consultez the section called "Exemples de clés de condition".

> **Note**
>
> Si vous utilisez une politique de compartiment pour appliquer des écritures conditionnelles, vous ne pouvez pas effectuer d'opérations de copie vers le compartiment ou le préfixe spécifié dans cette politique de compartiment. Les demandes `CopyObject` sans en-tête HTTP `If-None-Match` ou `If-Match` échouent avec une erreur `403 Access Denied`. Les demandes `CopyObject` effectuées avec ces en-têtes HTTP échouent avec une réponse `501 Not Implemented`.

Les exemples suivants montrent comment utiliser les conditions d'une politique de compartiment pour obliger les clients à utiliser l'en-tête HTTP `If-None-Match` ou `If-Match`.

Rubriques

- Exemple 1 : Autoriser uniquement les chargements d'objets à l'aide de demandes PutObject et CompleteMultipartUpload incluant l'en-tête if-none-match
- Exemple 2 : Autoriser uniquement les chargements d'objets à l'aide de demandes PutObject et CompleteMultipartUpload incluant l'en-tête if-match
- Exemple 3 : Autoriser uniquement les demandes de chargement d'objets incluant l'en-tête if-none-match ou if-match

Exemple 1 : Autoriser uniquement les chargements d'objets à l'aide de demandes **`PutObject`** et **`CompleteMultipartUpload`** incluant l'en-tête **`if-none-match`**

Cette politique permet au compte 111122223333, utilisateur Alice, d'écrire dans le *`amzn-s3-demo-bucket1`* compartiment si la demande inclut l'`if-none-match`en-tête, afin de s'assurer que la clé de l'objet n'existe pas déjà dans le compartiment. Toutes les demandes `PutObject` et `CompleteMultipartUpload` adressées au compartiment spécifié doivent inclure l'en-tête `if-none-match` pour aboutir. Avec cet en-tête, les clients ne peuvent écrire dans ce compartiment que si la clé d'objet n'existe pas dans le compartiment.

> **Note**
>
> Cette politique définit également la clé de `s3:ObjectCreationOperation` condition qui autorise les téléchargements partitionnés à l'aide des touches `CreateMultipartUploadUploadPart`, et. `UploadPartCopy` APIs

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowConditionalPut",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalPutwithMPUs",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        }
    ]
```

```
}
```

Exemple 2 : Autoriser uniquement les chargements d'objets à l'aide de demandes **`PutObject`** et **`CompleteMultipartUpload`** incluant l'en-tête **`if-match`**

Cette politique permet au compte 111122223333 et spécifiquement à l'utilisatrice Alice d'écrire dans *amzn-s3-demo-bucket1* uniquement si la demande inclut l'en-tête `if-match`. Cet en-tête compare la ETag valeur d'un objet dans S3 avec celle que vous avez fournie pendant l'`WRITE`opération. Si les ETag valeurs ne correspondent pas, l'opération échouera. Toutes les demandes `PutObject` et `CompleteMultipartUpload` adressées au compartiment spécifié doivent inclure l'en-tête `if-match` pour aboutir.

> **Note**
>
> Cette politique définit également la clé de `s3:ObjectCreationOperation` condition qui autorise les téléchargements partitionnés à l'aide des touches `CreateMultipartUploadUploadPart`, et. `UploadPartCopy` APIs

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObject",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
        },
        {
            "Sid": "BlockNonConditionalObjectCreation",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
```

```
                "Null": {
                    "s3:if-match": "true"
                },
                "Bool": {
                    "s3:ObjectCreationOperation": "true"
                }
            }
        },
        {
            "Sid": "AllowGetObjectBecauseConditionalPutIfMatchETag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

Exemple 3 : Autoriser uniquement les demandes de chargement d'objets incluant l'en-tête **`if-none-match`** ou **`if-match`**

Cette politique permet au compte 111122223333 et spécifiquement à l'utilisatrice Alice d'écrire dans *amzn-s3-demo-bucket1* si la demande inclut l'en-tête `if-none-match` ou `if-match`. Cela permet à Alice de télécharger un objet si le nom de clé n'existe pas dans le compartiment, ou si le nom de clé existe, Alice peut remplacer l'objet s'il ETag correspond à celui ETag fourni dans la PUT demande.

> **Note**
>
> Cette politique définit également la clé de `s3:ObjectCreationOperation` condition qui autorise les téléchargements partitionnés à l'aide des touches `CreateMultipartUploadUploadPart`, et. `UploadPartCopy` APIs

JSON

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

```
        {
            "Sid": " AllowConditionalPutifAbsent",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-none-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalPutIfMatchEtag",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Null": {
                    "s3:if-match": "false"
                }
            }
        },
        {
            "Sid": "AllowConditionalObjectCreation",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "Bool": {
                    "s3:ObjectCreationOperation": "false"
                }
            }
        },
        {
            "Sid": " AllowGetObjectBecauseConditionalPutIfMatchETag",
```

```
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Alice"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        }
    ]
}
```

Copie, déplacement et changement de nom des objets

L'`CopyObject`opération crée une copie d'un objet déjà stocké dans Amazon S3.

Vous pouvez créer une copie d'un objet d'une taille maximale de 5 Go dans une seule opération atomique. Toutefois, pour copier un objet dont la taille est supérieure à 5 Go, vous devez utiliser un téléchargement partitionné à l'aide du AWS CLI ou AWS SDKs. Pour de plus amples informations, veuillez consulter Copie d'un objet à l'aide du chargement partitionné.

> **Note**
>
> Pour conserver les avantages en termes de performances d'un objet que vous avez chargé à l'aide du téléchargement partitionné, vous devez copier l'objet à l'aide du téléchargement partitionné à l'aide du AWS SDK AWS CLI ou au lieu de la console S3. Pour de plus amples informations, veuillez consulter Copie d'un objet à l'aide du chargement partitionné.

Grâce à l'opération `CopyObject`, vous pouvez :

- Créez des copies supplémentaires d'objets.
- Renommez les objets en les copiant et en supprimant les originaux.
- Copiez ou déplacez des objets d'un compartiment à un autre, y compris entre Régions AWS (par exemple, entre `us-west-1` et `eu-west-2`). Lorsque vous déplacez un objet, Amazon S3 copie l'objet vers la destination spécifiée, puis supprime l'objet source.

> **Note**
>
> Le fait de copier ou de déplacer des objets Régions AWS entraîne des frais de bande passante. Pour plus d'informations, consultez Tarification Amazon S3.

- Modifiez les métadonnées d'objet. Chaque objet Amazon S3 possède des métadonnées. Ces métadonnées sont un ensemble de paires nom-valeur. Vous pouvez configurer les métadonnées d'un objet lorsque vous le chargez. Une fois que vous avez chargé l'objet, vous ne pouvez pas modifier les métadonnées de l'objet. Le seul moyen de modifier les métadonnées d'objet est de faire une copie de l'objet et de configurer les métadonnées. Pour ce faire, dans l'opération de copie, définissez le même objet comme source et cible.

  Certaines sont des métadonnées système et d'autres sont définies par l'utilisateur. Vous pouvez contrôler certaines métadonnées système. Par exemple, vous pouvez contrôler la classe de stockage et le type de chiffrement côté serveur à utiliser pour l'objet. Lorsque vous copiez un objet, les métadonnées système contrôlées par l'utilisateur et les métadonnées définies par l'utilisateur sont également copiées. Amazon S3 réinitialise les métadonnées contrôlées par le système. Par exemple, lorsque vous copiez un objet, Amazon S3 réinitialise la date de création de l'objet copié. Il est inutile de configurer les valeurs des ces métadonnées contrôlées par le système dans la demande de copie.

  Lorsque vous copiez un objet, vous devez choisir de mettre à jour certaines valeurs des métadonnées. Par exemple, si votre objet source est configuré pour utiliser le stockage S3 Standard, vous pouvez sélectionner S3 Intelligent-Tiering pour la copie de l'objet. Vous devez également choisir de modifier certaines valeurs des métadonnées définies par l'utilisateur présentes dans l'objet source. Si vous choisissez de mettre à jour les métadonnées (système ou définies par l'utilisateur) configurables par l'utilisateur de l'objet lors de la copie, vous devez explicitement spécifier toutes les métadonnées configurables par l'utilisateur présentes dans l'objet source de la demande, même si vous ne changez qu'une des valeurs des métadonnées.

  > **Note**
  >
  > Lorsque vous copiez un objet à l'aide de la console Amazon S3, vous pouvez recevoir le message d'erreur « Les métadonnées copiées ne peuvent pas être vérifiées ». La console utilise des en-têtes pour récupérer et définir les métadonnées de votre objet. Si la configuration de votre réseau ou de votre navigateur modifie vos requêtes réseau, ce comportement peut entraîner l'écriture involontaire de métadonnées (telles que `Cache-`

`Control` des en-têtes modifiés) dans l'objet copié. Amazon S3 ne peut pas vérifier ces métadonnées involontaires.
Pour résoudre ce problème, vérifiez la configuration de votre réseau et de votre navigateur pour vous assurer qu'elle ne modifie pas les en-têtes, tels que`Cache-Control`. Pour plus d'informations, consultez le modèle de responsabilité partagée.

Pour plus d'informations sur les métadonnées d'objet, consultez Utilisation des métadonnées d'objet.

Copie d'objets archivés et restaurés

Si l'objet source est archivé dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, vous devez d'abord restaurer une copie temporaire avant de copier l'objet vers un autre compartiment. Pour en savoir plus sur l'archivage des objets, consultez Utilisation des objets archivés.

L'opération Copier dans la console Amazon S3 n'est pas prise en charge pour les objets restaurés dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour copier ces objets restaurés, utilisez l'API REST AWS Command Line Interface (AWS CLI) AWS SDKs, ou l'API REST Amazon S3.

Copie d'objets chiffrés

Amazon S3 chiffre automatiquement tous les nouveaux objets copiés dans un compartiment S3. Si vous ne spécifiez aucune information de chiffrement dans votre demande de copie, le paramètre de chiffrement de l'objet cible est défini sur la configuration de chiffrement par défaut du compartiment de destination. Par défaut, tous les compartiments ont un niveau de chiffrement de base qui utilise le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3). Si le compartiment de destination possède une configuration de chiffrement par défaut qui utilise le chiffrement côté serveur avec une clé AWS Key Management Service (AWS KMS) (SSE-KMS) ou une clé de chiffrement fournie par le client (SSE-C), Amazon S3 utilise la clé KMS correspondante ou une clé fournie par le client pour chiffrer la copie de l'objet cible.

Lors de la copie d'un objet, si vous souhaitez utiliser un autre type de paramètre de chiffrement pour l'objet cible, vous pouvez demander à Amazon S3 de chiffrer l'objet cible à l'aide d'une clé KMS, d'une clé gérée par Amazon S3 ou d'une clé fournie par le client. Si le paramètre de chiffrement de votre demande est différent de la configuration de chiffrement par défaut du compartiment de destination, le paramètre de chiffrement de votre demande est prioritaire. Si l'objet source de la

copie est chiffré avec une clé SSE-C, vous devez fournir les informations de chiffrement nécessaires dans votre demande afin qu'Amazon S3 puisse déchiffrer l'objet à copier. Pour de plus amples informations, veuillez consulter Protection des données à l'aide du chiffrement.

Utilisation de sommes de contrôle lors de la copie d'objets

Lorsque vous copiez des objets, vous pouvez sélectionner un algorithme de total de contrôle différent pour l'objet. Que vous sélectionniez le même algorithme ou un nouvel algorithme, Amazon S3 calcule un nouveau total de contrôle après la copie de l'objet. Amazon S3 ne copie pas directement la valeur de la somme de contrôle. Tous les objets copiés sans spécification d'une somme de contrôle et d'algorithmes de somme de contrôle obtiennent automatiquement un algorithme de somme de contrôle `CRC-64NVME`. Pour plus d'informations sur le mode de calcul du total de contrôle, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Copie de plusieurs objets dans une seule demande

Pour copier plusieurs objets Amazon S3 avec une seule demande, vous pouvez utiliser la fonctionnalité d'opérations par lot S3. Vous fournissez à la fonctionnalité d'opérations par lots S3 une liste d'objets sur lesquels effectuer des opérations. La fonctionnalité des opérations par lot S3 appelle l'opération d'API respective pour effectuer l'opération spécifiée. Une tâche d'opérations par lot peut effectuer l'opération spécifiée sur des milliards d'objets contenant des exaoctets de données.

La fonctionnalité d'opérations par lot S3 suit la progression, envoie des notifications et stocke un rapport de fin détaillé sur toutes les actions, offrant ainsi une expérience sans serveur entièrement gérée et qui peut être vérifiée. Vous pouvez utiliser S3 Batch Operations via la console Amazon S3 ou AWS SDKs l'API REST. AWS CLI Pour de plus amples informations, veuillez consulter the section called "Principes de base des opérations par lot".

Copie d'objets dans des compartiments de répertoires

Pour plus d'informations sur la copie d'un objet dans un compartiment de répertoires, consultez Copie d'objets vers ou depuis un compartiment de répertoires. Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Pour copier un objet

Pour copier un objet, utilisez les méthodes suivantes.

Utilisation de la console S3

> **Note**
>
> Voici les restrictions et limites qui s'appliquent lorsque vous copiez un objet avec la console :
>
> - Vous pouvez copier un objet si sa taille est inférieure à 5 Go. Si la taille de votre objet est supérieure à 5 Go, vous devez utiliser le AWS CLIou AWS SDKspour copier un objet.
> - Pour obtenir la liste des autorisations supplémentaires requises pour copier des objets, consultez the section called "Autorisations requises pour les opérations d'API S3". Pour obtenir un exemple de politiques qui accorde ces autorisations, consultez the section called "Exemples de politiques basées sur l'identité".
> - L'action Copy s'applique à tous les objets des dossiers spécifiés (préfixes). Les objets ajoutés à ces dossiers pendant que l'action est en cours risquent d'être affectés.
> - La copie interrégionale d'objets chiffrés avec SSE-KMS n'est pas prise en charge par la console Amazon S3. Pour copier des objets chiffrés avec SSE-KMS d'une région à l'autre AWS CLI, utilisez le AWS SDK ou l'API REST Amazon S3.
> - Les objets chiffrés avec des clés de chiffrement fournies par le client (SSE-C) ne peuvent pas être copiés à l'aide de la console S3. Pour copier des objets chiffrés avec SSE-C, utilisez le AWS CLI AWS SDK ou l'API REST Amazon S3.
> - Les objets copiés ne conservent pas les paramètres de verrouillage des objets d'origine.
> - Si le compartiment à partir duquel vous copiez des objets utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, l'objet ne ACLs sera pas copié vers la destination spécifiée.
> - Si vous souhaitez copier des objets dans un compartiment qui utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, assurez-vous que le compartiment source utilise également le paramètre imposé par le propriétaire du compartiment, ou supprimez tout objet accordé par l'ACL à d'autres AWS comptes et groupes.

Pour copier un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant les objets que vous souhaitez copier.
4. Cochez la case située à gauche du nom des objets que vous souhaitez copier.
5. Dans le menu Actions, choisissez Copier à partir de la liste d'options qui s'affiche.
6. Sélectionnez le type de destination et le compte de destination. Pour spécifier le chemin de destination, choisissez Browse S3 (Parcourir S3), accédez à la destination et activez la case à cocher située à gauche de la destination. Choisissez Choose destination (Choisir une destination) en bas à droite.

   Vous pouvez également saisir le chemin de destination.
7. Si la gestion des versions n'est pas activée au niveau des compartiments, un avertissement vous recommande de l'activer afin de vous protéger contre le remplacement ou la suppression involontaires d'objets. Si vous souhaitez conserver toutes les versions des objets dans ce compartiment, sélectionnez Enable Bucket Versioning (Activer la gestion des versions pour le compartiment). Vous pouvez également consulter les propriétés de chiffrement et de verrouillage d'objet S3 par défaut dans Détails de la destination.
8. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.
9. En bas à droite, choisissez Copy (Copier). Amazon S3 copie votre objet dans la destination.

À l'aide du AWS SDKs

Les exemples de cette section vous montrent comment copier des objets supérieurs à 5 Go en une seule opération. Pour copier les objets supérieurs à 5 Go, vous devez utiliser un chargement partitionné. Pour de plus amples informations, veuillez consulter Copie d'un objet à l'aide du chargement partitionné.

Java

Example

L'exemple suivant copie un objet dans Amazon S3 à l'aide du kit AWS SDK pour Java. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;

import java.io.IOException;

public class CopyObjectSingleOperation {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String sourceKey = "*** Source object key *** ";
        String destinationKey = "*** Destination object key ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Copy the object into a new object in the same bucket.
            CopyObjectRequest copyObjRequest = new CopyObjectRequest(bucketName,
 sourceKey, bucketName, destinationKey);
            s3Client.copyObject(copyObjRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
```

```
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

L'exemple C# suivant utilise le niveau élevé SDK pour .NET pour copier des objets d'une taille maximale de 5 Go en une seule opération. Pour les objets de taille supérieurs à 5 Go, utilisez l'exemple de copie de chargement partitionné décrit dans Copie d'un objet à l'aide du chargement partitionné.

Cet exemple effectue la copie d'un objet de 5 Go au plus. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CopyObjectTest
    {
        private const string sourceBucket = "*** provide the name of the bucket with
 source object ***";
        private const string destinationBucket = "*** provide the name of the bucket
 to copy the object to ***";
        private const string objectKey = "*** provide the name of object to copy
 ***";
        private const string destObjectKey = "*** provide the destination object key
 name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
```

```
        {
            s3Client = new AmazonS3Client(bucketRegion);
            Console.WriteLine("Copying an object");
            CopyingObjectAsync().Wait();
        }

        private static async Task CopyingObjectAsync()
        {
            try
            {
                CopyObjectRequest request = new CopyObjectRequest
                {
                    SourceBucket = sourceBucket,
                    SourceKey = objectKey,
                    DestinationBucket = destinationBucket,
                    DestinationKey = destObjectKey
                };
                CopyObjectResponse response = await
 s3Client.CopyObjectAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

Cette rubrique explique comment utiliser les classes de la version 3 de AWS SDK pour PHP pour copier un seul objet et plusieurs objets au sein d'Amazon S3, d'un compartiment à un autre ou au sein du même compartiment.

Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

L'exemple PHP suivant illustre l'utilisation de la méthode `copyObject()` pour copier un seul objet dans Amazon S3. Il montre également comment créer plusieurs copies d'un objet en utilisant un lot d'appels de `CopyObject` avec la méthode `getcommand()`.

Copie d'objets

1	Créez l'instance d'un client Simple Storage Service (Amazon S3) à l'aide du constructeur de classe `Aws\S3\S3Client` .
2	Pour créer plusieurs copies d'un objet, exécutez un lot d'appels à la méthode getCommand() du client Amazon S3, qui est héritée de la classe Aws\CommandInterface. Vous fournissez la commande `CopyObject` comme le premier argument et un tableau contenant le compartiment source, le nom de la clé source, le compartiment cible et le nom de la clé cible comme second argument.

```
 require 'vendor/autoload.php';

use Aws\CommandPool;
use Aws\Exception\AwsException;
use Aws\ResultInterface;
use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';
$targetBucket = '*** Your Target Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region' => 'us-east-1'
]);

// Copy an object.
$s3->copyObject([
    'Bucket' => $targetBucket,
    'Key' => "$sourceKeyname-copy",
    'CopySource' => "$sourceBucket/$sourceKeyname",
]);

// Perform a batch of CopyObject operations.
$batch = array();
for ($i = 1; $i <= 3; $i++) {
```

```
    $batch[] = $s3->getCommand('CopyObject', [
        'Bucket' => $targetBucket,
        'Key' => "{targetKeyname}-$i",
        'CopySource' => "$sourceBucket/$sourceKeyname",
    ]);
}
try {
    $results = CommandPool::batch($s3, $batch);
    foreach ($results as $result) {
        if ($result instanceof ResultInterface) {
            // Result handling here
        }
        if ($result instanceof AwsException) {
            // AwsException handling here
        }
    }
} catch (Exception $e) {
    // General error handling here
}
```

Python

```
class ObjectWrapper:
    """Encapsulates S3 object actions."""

    def __init__(self, s3_object):
        """
        :param s3_object: A Boto3 Object resource. This is a high-level resource in
 Boto3
                          that wraps object actions in a class-like structure.
        """
        self.object = s3_object
        self.key = self.object.key
```

```
    def copy(self, dest_object):
        """
        Copies the object to another bucket.

        :param dest_object: The destination object initialized with a bucket and
 key.
                            This is a Boto3 Object resource.
```

```
        """
        try:
            dest_object.copy_from(
                CopySource={"Bucket": self.object.bucket_name, "Key":
self.object.key}
            )
            dest_object.wait_until_exists()
            logger.info(
                "Copied object from %s:%s to %s:%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
        except ClientError:
            logger.exception(
                "Couldn't copy object from %s/%s to %s/%s.",
                self.object.bucket_name,
                self.object.key,
                dest_object.bucket_name,
                dest_object.key,
            )
            raise
```

Ruby

Les tâches suivantes vous guident tout au long de l'utilisation des classes Ruby pour copier un objet dans Amazon S3, d'un compartiment à un autre ou au sein d'un même compartiment.

Copie d'objets

1	Utilisez la gemme modulaire Amazon S3 pour la version 3 de AWS SDK pour Ruby`aws-sdk-s3` , exigez et fournissez vos AWS informations d'identification. Pour plus d'informations sur la manière de fournir vos informations d'identif ication, consultez la section Faire des demandes à l'aide des informations d'identif ication d'un AWS compte ou d'un utilisateur IAM dans le manuel Amazon S3 API Reference.
2	Fournissez les informations de la demande comme le nom du compartiment source, le nom de la clé source, le nom du compartiment cible et la clé de destination.

L'exemple de code Ruby suivant présente les tâches précédentes grâce à la méthode `#copy_object` permettent de copier un objet d'un compartiment à un autre.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
  #                                        copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket and rename it with the
 target key.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
```

```
  target_object = wrapper.copy_object(target_bucket, target_key)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Utilisation de l'API REST

Cet exemple décrit comment copier un objet à l'aide de l'API REST Amazon S3. Pour plus d'informations sur l'API REST, consultez CopyObject.

L'exemple copie l'objet `flotsam` du compartiment *amzn-s3-demo-bucket1* vers l'objet `jetsam` du compartiment *amzn-s3-demo-bucket2*, en préservant les métadonnées.

```
PUT /jetsam HTTP/1.1
Host: amzn-s3-demo-bucket2.s3.amazonaws.com
x-amz-copy-source: /amzn-s3-demo-bucket1/flotsam
Authorization: AWS AKIAIOSFODNN7EXAMPLE:ENoSbxYByFA0UGLZUqJN5EUnLDg=
Date: Wed, 20 Feb 2008 22:12:21 +0000
```

La signature est générée à partir des informations suivantes.

```
PUT\r\n
\r\n
\r\n
Wed, 20 Feb 2008 22:12:21 +0000\r\n

x-amz-copy-source:/amzn-s3-demo-bucket1/flotsam\r\n
/amzn-s3-demo-bucket2/jetsam
```

Amazon S3 renvoie la réponse suivante qui indique ETag l'objet et la date de sa dernière modification.

```
HTTP/1.1 200 OK
x-amz-id-2: Vyaxt7qEbzv34BnSu5hctyyNSlHTYZFMWK4FtzO+iX8JQNyaLdTshL0KxatbaOZt
x-amz-request-id: 6B13C3C5B34AF333
Date: Wed, 20 Feb 2008 22:13:01 +0000
```

```
Content-Type: application/xml
Transfer-Encoding: chunked
Connection: close
Server: AmazonS3
<?xml version="1.0" encoding="UTF-8"?>

<CopyObjectResult>
   <LastModified>2008-02-20T22:13:01</LastModified>
   <ETag>"7e9c608af58950deeb370c98608ed097"</ETag>
</CopyObjectResult>
```

À l'aide du AWS CLI

Vous pouvez également utiliser le AWS Command Line Interface (AWS CLI) pour copier un objet S3. Pour plus d'informations, consultez copy-object dans la Référence des commandes de l'AWS CLI .

Pour plus d'informations sur le AWS CLI, voir Qu'est-ce que le AWS Command Line Interface ? dans le guide de AWS Command Line Interface l'utilisateur.

Pour déplacer un objet

Pour déplacer un objet, utilisez les méthodes suivantes.

Utilisation de la console S3

> **Note**
>
> - Vous pouvez déplacer un objet si sa taille est inférieure à 5 Go. Si la taille de votre objet est supérieure à 5 Go, vous devez utiliser le AWS CLIou AWS SDKspour déplacer un objet.
> - Pour obtenir la liste des autorisations supplémentaires requises pour déplacer des objets, consultez the section called "Autorisations requises pour les opérations d'API S3". Pour obtenir un exemple de politiques qui accorde ces autorisations, consultez the section called "Exemples de politiques basées sur l'identité".
> - Les objets chiffrés à l'aide des clés de chiffrement fournies par le client (SSE-C) ne peuvent pas être déplacés à l'aide de la console Amazon S3. Pour déplacer des objets chiffrés avec SSE-C, utilisez l' AWS CLI API REST AWS SDKs, ou Amazon S3.
> - Lorsque vous déplacez des dossiers, attendez la fin de l'opération Déplacer pour apporter des modifications supplémentaires dans les dossiers.

- Vous ne pouvez pas utiliser les alias de point d'accès S3 comme source ou destination pour les opérations Déplacer dans la console Amazon S3.

Pour déplacer un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments. Accédez au compartiment ou au dossier Amazon S3 contenant les objets que vous souhaitez déplacer.
3. Cochez la case située à côté de l'objet que vous souhaitez déplacer.
4. Dans le menu Actions, choisissez Déplacer.
5. Pour spécifier le chemin de destination, choisissez Parcourir S3, accédez à la destination et cochez la case située à gauche de la destination. Choisissez Choose destination (Choisir une destination).

   Vous pouvez également saisir le chemin de destination.
6. Si la gestion des versions n'est pas activée au niveau des compartiments, un avertissement vous recommande de l'activer afin de vous protéger contre le remplacement ou la suppression involontaires d'objets. Si vous souhaitez conserver toutes les versions des objets dans ce compartiment, sélectionnez Enable Bucket Versioning (Activer la gestion des versions pour le compartiment). Vous pouvez également consulter les propriétés de chiffrement et de verrouillage des objets par défaut dans Détails de la destination.
7. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.
8. En bas à droite, choisissez Move (Déplacer). Amazon S3 déplace vos objets vers la destination.

À l'aide du AWS CLI

Vous pouvez également utiliser le AWS Command Line Interface (AWS CLI) pour déplacer un objet S3. Pour plus d'informations, consultez mv dans la Référence des commandes de l'AWS CLI .

Pour plus d'informations sur le AWS CLI, voir Qu'est-ce que le AWS Command Line Interface ? dans le guide de AWS Command Line Interface l'utilisateur.

Pour renommer un objet

Pour renommer un objet, utilisez la procédure suivante.

> **Note**
>
> - Vous pouvez renommer un objet si sa taille est inférieure à 5 Go. Pour renommer des objets de plus de 5 Go, vous devez utiliser le AWS CLIou AWS SDKspour copier votre objet sous un nouveau nom, puis supprimer l'objet d'origine.
> - Pour obtenir la liste des autorisations supplémentaires requises pour copier des objets, consultez the section called "Autorisations requises pour les opérations d'API S3". Pour obtenir un exemple de politiques qui accorde ces autorisations, consultez the section called "Exemples de politiques basées sur l'identité".
> - Le changement de nom d'un objet crée une copie de cet objet avec une nouvelle date de dernière modification, puis ajoute un marqueur de suppression à l'objet d'origine.
> - Les paramètres du bucket pour le chiffrement par défaut sont automatiquement appliqués à tout objet spécifié qui n'est pas chiffré.
> - Vous ne pouvez pas utiliser la console Amazon S3 pour renommer des objets à l'aide de clés de chiffrement fournies par le client (SSE-C). Pour renommer des objets chiffrés avec SSE-C, utilisez l'API REST AWS CLI AWS SDKs, ou Amazon S3 pour copier ces objets sous un nouveau nom.
> - Si ce compartiment utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, les listes de contrôle d'accès aux objets (ACLs) ne seront pas copiées.

Pour renommer un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments, puis l'onglet Compartiments à usage général. Accédez au compartiment ou au dossier Amazon S3 contenant l'objet que vous souhaitez renommer.

3. Cochez la case située à côté de l'objet que vous voulez renommer.
4. Dans le menu Actions, sélectionnez Renommer l'objet.
5. Dans la zone Nouveau nom d'objet, saisissez le nouveau nom de l'objet.
6. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.
7. Sélectionnez Enregistrer les modifications. Amazon S3 renommera votre objet.

Téléchargement d'objets

Cette section explique comment télécharger des objets depuis un compartiment Amazon S3. Avec Amazon S3, vous pouvez stocker des objets dans un ou plusieurs compartiments, et chaque objet peut atteindre une taille de 5 To. Tout objet Amazon S3 non archivé est accessible en temps réel. Les objets archivés doivent toutefois être restaurés avant de pouvoir être téléchargés. Pour obtenir des informations sur le téléchargement des objets archivés, consultez the section called "Téléchargement des objets archivés".

Vous pouvez télécharger un seul objet à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs Pour télécharger un objet depuis S3 sans écrire de code ni exécuter aucune commande, utilisez la console S3. Pour de plus amples informations, veuillez consulter the section called "Téléchargement d'un objet".

Pour télécharger plusieurs objets AWS CloudShell, utilisez le AWS CLI ou le AWS SDKs. Pour de plus amples informations, veuillez consulter the section called "Téléchargement de plusieurs objets".

Si vous devez télécharger une partie d'un objet, vous devez utiliser des paramètres supplémentaires avec l'API REST AWS CLI ou pour spécifier uniquement les octets que vous souhaitez télécharger. Pour de plus amples informations, veuillez consulter the section called "Téléchargement d'une partie d'un objet".

Si vous devez télécharger un objet qui ne vous appartient pas, demandez à son propriétaire de générer une URL présignée qui vous permettra de télécharger l'objet. Pour de plus amples informations, veuillez consulter the section called "Téléchargement d'un objet à partir d'un autre Compte AWS".

Lorsque vous téléchargez des objets en dehors du AWS réseau, des frais de transfert de données s'appliquent. Le transfert de données au sein du AWS réseau est gratuit Région AWS, mais toute `GET` demande vous sera facturée. Pour plus d'informations sur les coûts de transfert de données et les frais de récupération de données, consultez Tarification Amazon S3.

Rubriques

- Téléchargement d'un objet
- Téléchargement de plusieurs objets
- Téléchargement d'une partie d'un objet
- Téléchargement d'un objet à partir d'un autre Compte AWS
- Téléchargement des objets archivés
- Téléchargement d'objets en fonction des métadonnées
- Résolution des problèmes de téléchargement d'objets

Téléchargement d'un objet

Vous pouvez télécharger un objet à l'aide de la console Amazon S3 ou de AWS SDKs l'API REST. AWS CLI

Utilisation de la console S3

Cette section explique comment utiliser la console Amazon S3 pour télécharger un objet depuis un compartiment S3.

> **Note**
>
> - Vous ne pouvez télécharger qu'un seul objet à la fois.
> - Si vous utilisez la console Amazon S3 pour télécharger un objet dont le nom de clé se termine par un point (`.`), celui-ci est supprimé du nom de clé de l'objet téléchargé. Pour conserver le délai à la fin du nom de l'objet téléchargé, vous devez utiliser l'API REST AWS Command Line Interface (AWS CLI) ou Amazon S3. AWS SDKs

Pour télécharger un objet à partir d'un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment à partir duquel vous souhaitez télécharger un objet.
4. Vous pouvez télécharger un objet à partir d'un compartiment S3 de l'une des façons suivantes :
   - Cochez la case à côté de l'objet et choisissez Télécharger. Si vous souhaitez télécharger l'objet dans un dossier spécifique, dans le menu Actions, choisissez Télécharger en tant que.
   - Si vous souhaitez télécharger une version spécifique de l'objet, activez Afficher les versions (en regard de la zone de recherche). Cochez la case à côté de la version de l'objet de votre choix, puis choisissez Télécharger. Si vous souhaitez télécharger l'objet dans un dossier spécifique, dans le menu Actions, choisissez Télécharger en tant que.

À l'aide du AWS CLI

L'exemple de commande `get-object` suivant montre comment utiliser l'interface AWS CLI pour télécharger un objet depuis Amazon S3. Cette commande récupère l'objet *`folder/my_image`* à partir du compartiment *`amzn-s3-demo-bucket1`*. Vous devez inclure un`outfile`, qui est le nom de fichier de l'objet téléchargé, tel que*`my_downloaded_image.jpg`*.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/
my_image my_downloaded_image.jpg
```

Pour plus d'informations et des exemples, consultez get-object dans la Référence des commandes de l'AWS CLI .

À l'aide du AWS SDKs

Pour des exemples de téléchargement d'un objet avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour récupérer des objets depuis Amazon S3. Pour plus d'informations, consultez GetObject dans la Référence d'API Amazon Simple Storage Service.

Téléchargement de plusieurs objets

Vous pouvez télécharger plusieurs objets en utilisant le AWS CloudShell AWS CLI, ou le AWS SDKs.

En utilisant AWS CloudShell dans AWS Management Console

AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console

Pour plus d'informations AWS CloudShell, voir Qu'est-ce que c'est CloudShell ? dans le guide de AWS CloudShell l'utilisateur.

> **Important**
>
> Avec AWS CloudShell, votre répertoire personnel dispose d'un espace de stockage allant jusqu'à 1 Go par. Région AWS Par conséquent, vous ne pouvez pas synchroniser les compartiments avec des objets dont le total est supérieur à ce montant. Pour plus de restrictions, consultez Quotas et restrictions des services dans le Guide de l'utilisateur AWS CloudShell .

Pour télécharger des objets en utilisant AWS CloudShell

1. Connectez-vous à la CloudShell console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudshell/.
2. Exécutez la commande suivante pour synchroniser les objets de votre bucket avec CloudShell. La commande suivante synchronise les objets du compartiment nommé *amzn-s3-demo-bucket1* et crée un dossier nommé *temp* dans CloudShell. CloudShell synchronise vos objets dans ce dossier. Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3 sync s3://amzn-s3-demo-bucket1 ./temp
```

> **Note**
>
> La `sync` commande n'est pas compatible avec les compartiments de répertoire. Pour effectuer une correspondance de modèles afin d'exclure ou d'inclure des objets particuliers, vous pouvez utiliser les paramètres `--exclude "value"` et `--include "value"` avec la commande `sync`.

3. Exécutez la commande suivante pour compresser vos objets dans le dossier nommé *temp* dans un fichier nommé *temp.zip*.

```
zip temp.zip -r temp/
```

4. Choisissez Actions, puis choisissez Télécharger un fichier.
5. Entrez le nom de fichier **temp.zip**, puis choisissez Télécharger.
6. (Facultatif) Supprimez le *temp.zip* fichier et les objets synchronisés avec le *temp* dossier dans CloudShell. Avec AWS CloudShell, vous disposez d'un stockage persistant allant jusqu'à 1 Go pour chaque Région AWS.

   Vous pouvez utiliser l'exemple de commande suivant pour supprimer votre fichier `.zip` et votre dossier. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
rm temp.zip && rm -rf temp/
```

À l'aide du AWS CLI

L'exemple suivant montre comment vous pouvez utiliser le AWS CLI pour télécharger tous les fichiers ou objets du répertoire ou du préfixe spécifié. Cette commande copie tous les objets du compartiment *amzn-s3-demo-bucket1* vers votre répertoire actuel. Pour utiliser cet exemple de commande, utilisez le nom de votre compartiment à la place de *amzn-s3-demo-bucket1*.

```
aws s3 cp s3://amzn-s3-demo-bucket1 . --recursive
```

La commande suivante télécharge tous les objets situés sous le préfixe *logs* du compartiment *amzn-s3-demo-bucket1* dans votre répertoire actuel. Elle utilise également les paramètres `--`

`exclude` et `--include` pour copier uniquement les objets dotés du suffixe *`.log`*. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3 cp s3://amzn-s3-demo-bucket1/logs/ . --recursive --exclude "*" --include "*.log"
```

Pour plus d'informations et des exemples, consultez cp dans la Référence des commandes AWS CLI .

À l'aide du AWS SDKs

Pour des exemples de téléchargement de tous les objets d'un compartiment Amazon S3 avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Téléchargement d'une partie d'un objet

Vous pouvez télécharger une partie d'un objet à l'aide de l' AWS CLI API REST. Pour ce faire, vous devez utiliser des paramètres supplémentaires pour spécifier la partie d'un objet que vous souhaitez télécharger.

À l'aide du AWS CLI

L'exemple de commande suivant exécute une demande `GET` pour obtenir une plage d'octets dans l'objet nommé *`folder/my_data`* dans le compartiment nommé *`amzn-s3-demo-bucket1`*. Dans cette demande, la plage d'octets doit être préfixée par `bytes=`. L'objet partiel est téléchargé dans le fichier de sortie nommé *`my_data_range`*. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --key folder/my_data --range
 bytes=0-500 my_data_range
```

Pour plus d'informations et des exemples, consultez get-object dans la Référence des commandes AWS CLI .

Pour plus d'informations sur l'en-tête HTTP `Range`, consultez RFC 9110 sur le site web RFC Editor.

> **Note**
>
> Amazon S3 ne prend pas en charge la récupération de plusieurs plages de données dans une demande `GET` individuelle.

Utilisation de l'API REST

Vous pouvez utiliser les paramètres `partNumber` et `Range` de l'API REST pour récupérer des parties d'objet depuis Amazon S3. Pour plus d'informations, consultez GetObject dans la Référence d'API Amazon Simple Storage Service.

Téléchargement d'un objet à partir d'un autre Compte AWS

Vous pouvez utiliser une URL présignée pour accorder aux autres un accès limité dans le temps à vos objets sans mettre à jour votre politique de compartiment.

L'URL présignée peut être saisie dans un navigateur ou utilisée par un programme pour télécharger un objet. Les informations d'identification utilisées par l'URL sont celles de l' AWS utilisateur qui a généré l'URL. Une fois l'URL créée, toute personne disposant de l'URL présignée peut télécharger l'objet correspondant jusqu'à ce que l'URL expire.

Utilisation d'une URL présignée dans la console S3

Vous pouvez utiliser la console Amazon S3 pour générer une URL présignée afin de partager un objet dans un compartiment à usage général en suivant ces étapes. Dans la console, le délai d'expiration maximal d'une URL présignée est de 12 heures à compter de la création.

Pour générer une URL présignée à l'aide de la console Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant l'objet pour lequel vous souhaitez obtenir une URL présignée.
4. Dans la liste Objects (Objets), sélectionnez l'objet pour lequel vous souhaitez créer une URL présignée.
5. Dans le menu Actions d'objet, choisissez Partager avec une URL présignée.

6. Spécifiez la durée de validité souhaitée pour l'URL présignée.
7. Choisissez Create presigned URL (Créer une URL présignée).
8. Lorsqu'un message de confirmation apparaît, l'URL est automatiquement copiée dans votre presse-papier. Un bouton s'affiche pour copier l'URL présignée, si vous devez la copier à nouveau.
9. Pour télécharger l'objet, collez l'URL dans n'importe quel navigateur et l'objet tentera de se télécharger.

Pour plus d'informations sur les méthodes présignées URLs et les autres méthodes permettant de les créer, consultezTéléchargez et chargez des objets avec une signature préalable URLs.

Téléchargement des objets archivés

Pour réduire vos coûts de stockage pour les objets rarement consultés, vous pouvez archiver ces objets. Lorsque vous archivez un objet, il est placé dans un espace de stockage à faible coût, ce qui signifie que vous ne pouvez pas y accéder en temps réel. Pour télécharger un objet archivé, vous devez d'abord le restaurer.

Vous pouvez restaurer les objets archivés en quelques minutes ou quelques heures, selon la classe de stockage. Vous pouvez restaurer un objet archivé à l'aide de la console Amazon S3, de S3 Batch Operations, de l'API REST Amazon S3 AWS SDKs, du, et du AWS Command Line Interface (AWS CLI).

Pour obtenir des instructions, veuillez consulter Restauration d'un objet archivé. Après avoir restauré l'objet archivé, vous pouvez le télécharger.

Téléchargement d'objets en fonction des métadonnées

Vous pouvez ajouter des conditions préalables pour télécharger un objet en fonction de ses métadonnées à l'aide d'une demande de lecture conditionnelle. Vous pouvez renvoyer un objet en fonction de sa balise Entity (ETag) ou de sa date de dernière modification. Cela permet limiter une opération S3 aux objets mis à jour depuis une date spécifiée ou de ne renvoyer qu'une version d'objet spécifique.

Vous pouvez utiliser des écritures conditionnelles pour les demandes GetObject ou HeadObject.

Pour plus d'informations sur les demandes conditionnelles, consultez Ajout de conditions préalables aux opérations S3 avec des demandes conditionnelles.

Résolution des problèmes de téléchargement d'objets

Des autorisations insuffisantes ou des politiques de bucket ou d'utilisateur AWS Identity and Access Management (IAM) incorrectes peuvent provoquer des erreurs lorsque vous essayez de télécharger des objets depuis Amazon S3. Ces problèmes peuvent souvent provoquer des erreurs d'accès refusé (403 Forbidden), quand Amazon S3 ne parvient pas à autoriser l'accès à une ressource.

Pour connaître les causes courantes des erreurs d'accès refusé (403 Forbidden), consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3.

Si vous recevez une NoSuchKey erreur 404 lorsque vous tentez d'accéder à un objet, consultez Comment puis-je résoudre le problème lié à l' NoSuchKey erreur 404 d'Amazon S3 ? dans le AWS re:Post Knowledge Center.

Vérification de l'intégrité des objets dans Amazon S3

Amazon S3 utilise des valeurs de somme de contrôle pour vérifier l'intégrité des données que vous chargez ou téléchargez. En outre, vous pouvez demander qu'un autre total de contrôle soit calculé pour tout objet que vous stockez dans Amazon S3. Vous pouvez choisir un algorithme de somme de contrôle à utiliser lors du chargement, de la copie standard ou de la copie par lot de vos données.

Lorsque vous chargez vos données, Amazon S3 utilise l'algorithme que vous avez choisi pour calculer une somme de contrôle côté serveur et la valide avec la valeur fournie avant de stocker l'objet et de stocker la somme de contrôle dans le cadre des métadonnées de l'objet. Cette validation fonctionne de manière cohérente quels que soient les modes de chiffrement, les tailles d'objets et les classes de stockage pour les chargements en une seule partie ou les chargements partitionnés. Cependant, lorsque vous copiez vos données de manière standard ou par lot, Amazon S3 calcule la somme de contrôle de l'objet source et la transfère vers l'objet de destination.

> **Note**
>
> Lorsque vous effectuez un chargement en une seule partie ou un chargement partitionné, vous pouvez intégrer une somme de contrôle précalculée à votre demande et utiliser le type de somme de contrôle de l'objet entier. Pour utiliser des valeurs précalculées avec plusieurs objets, utilisez le ou. AWS CLI AWS SDKs

Utilisation des algorithmes de total de contrôle pris en charge

Avec Amazon S3, vous pouvez choisir un algorithme de somme de contrôle pour valider vos données lors des chargements. L'algorithme de somme de contrôle spécifié est ensuite stocké avec l'objet et peut être utilisé pour valider l'intégrité des données lors des chargements. Vous pouvez sélectionner l'un des algorithmes suivants de somme de contrôle Secure Hash Algorithms (SHA) ou Cyclic Redundancy Check (CRC) pour calculer la valeur de la somme de contrôle :

- CRC-64/NVME () `CRC64NVME`
- CRC-32 () `CRC32`
- CRC-32C () `CRC32C`
- SHA-1 () `SHA1`
- SHA-256 () `SHA256`

En outre, vous pouvez fournir une somme de contrôle pour chaque demande à l'aide de l'MD5en-tête Content-.

Lorsque vous chargez un objet, vous spécifiez l'algorithme que vous souhaitez utiliser :

- Lorsque vous utilisez le AWS Management Console, choisissez l'algorithme de somme de contrôle que vous souhaitez utiliser. Vous avez la possibilité de spécifier la valeur de la somme de contrôle de l'objet. Lorsque Amazon S3 reçoit l'objet, il calcule le total de contrôle en utilisant l'algorithme que vous avez spécifié. Si les deux valeurs ne correspondent pas, Amazon S3 génère une erreur.
- Lorsque vous utilisez un kit SDK, gardez à l'esprit les points suivants :
  - Définissez le paramètre `ChecksumAlgorithm` selon l'algorithme que vous souhaitez qu'Amazon S3 utilise. Si vous disposez déjà d'une somme de contrôle précalculée, vous transmettez la valeur de la somme de contrôle au AWS SDK, qui inclut la valeur dans la demande. Si vous ne transmettez pas de valeur de somme de contrôle ou ne spécifiez pas d'algorithme de somme de contrôle, le kit SDK calculera automatiquement une valeur de somme de contrôle pour vous et l'inclura dans la demande afin de fournir des protections d'intégrité. Si la valeur de somme de contrôle individuelle ne correspond pas à la valeur définie par l'algorithme de somme de contrôle, Amazon S3 abandonne la demande avec une erreur `BadDigest`.
  - Si vous utilisez un AWS SDK mis à jour, celui-ci choisit un algorithme de somme de contrôle pour vous. Vous pouvez toutefois remplacer cet algorithme.

- Si vous ne spécifiez pas d'algorithme de somme de contrôle et que le SDK ne calcule pas non plus de somme de contrôle pour vous, S3 choisit automatiquement l'algorithme de somme de contrôle CRC-64/NVME (). `CRC64NVME`

- Lorsque vous utilisez l'API REST, n'utilisez pas le paramètre `x-amz-sdk-checksum-algorithm`. Utilisez plutôt l'un des en-têtes spécifiques à l'algorithme (par exemple, `x-amz-checksum-crc32`).

Pour appliquer ces valeurs de somme de contrôle à des objets déjà chargés sur Amazon S3, vous pouvez copier l'objet et spécifier si vous voulez utiliser l'algorithme de somme de contrôle existant ou un autre. Si vous ne spécifiez aucun algorithme, S3 utilise l'algorithme existant. Si l'objet source ne possède pas d'algorithme de somme de contrôle ou de valeur de somme de contrôle spécifié, Amazon S3 utilise l'algorithme CRC-64/NVME pour calculer la valeur de somme de contrôle pour l'objet de destination. Vous pouvez spécifier un algorithme de somme de contrôle lors de la copie d'objets à l'aide des opérations par lot S3.

> **Important**
>
> Si vous utilisez un chargement partitionné avec des sommes de contrôle pour des sommes de contrôle composites (ou au niveau des parties), les numéros de pièce du téléchargement partitionné doivent être consécutifs et commencer par 1. Si vous essayez de finaliser une demande de chargement partitionné avec des numéros de partie non consécutifs, Amazon S3 génère une erreur `HTTP 500 Internal Server`.

Types de sommes de contrôle d'objet entier et composites

Dans Amazon S3, deux types de sommes de contrôle sont pris en charge :

- Sommes de contrôle des objets entiers : la somme de contrôle d'un objet entier est calculée sur la base de l'ensemble du contenu d'un chargement partitionné, couvrant toutes les données allant du premier octet de la première partie chargée au dernier octet de la dernière partie chargée.

  > **Note**
  >
  > Toutes les demandes PUT nécessitent un type de somme de contrôle d'objet entier.

- Sommes de contrôle composites : une somme de contrôle composite est calculée sur la base des sommes de contrôle individuelles de chaque partie d'un chargement partitionné. Au lieu de calculer une somme de contrôle basée sur l'ensemble du contenu des données, cette approche agrège les sommes de contrôle au niveau de chaque partie (de la première à la dernière) afin de générer une somme de contrôle unique combinée pour l'objet entier.

> **Note**
>
> Lorsqu'un objet est chargé en plusieurs parties, la balise d'entité (ETag) de l'objet n'est pas un MD5 condensé de l'objet dans son intégralité. Amazon S3 calcule plutôt le MD5 résumé de chaque partie individuelle au fur et à mesure de son chargement. Les MD5 résumés sont utilisés pour déterminer l' ETag objet final. Amazon S3 concatène les octets des MD5 résumés, puis calcule le MD5 condensé de ces valeurs concaténées. Au cours de la dernière étape de ETag création, Amazon S3 ajoute un tiret indiquant le nombre total de pièces jusqu'à la fin.

Amazon S3 prend en charge les types de sommes de contrôle d'objet entier et les types de sommes de contrôle composites suivants :

- CRC-64/NVME (`CRC64NVME`) : Supporte uniquement le type d'algorithme d'objet complet.
- CRC-32 (`CRC32`) : Supporte à la fois les types d'objets complets et les types d'algorithmes composites.
- CRC-32C (`CRC32C`) : Supporte à la fois les types d'objets complets et les types d'algorithmes composites.
- SHA-1 (`SHA1`) : Supporte à la fois les types d'objets complets et les types d'algorithmes composites.
- SHA-256 (`SHA256`) : Supporte à la fois les types d'objets complets et les types d'algorithmes composites.

> **Note**
>
> Si vous utilisez un algorithme `SHA-1` ou un algorithme de `SHA-256` somme de contrôle pour un téléchargement partitionné, vous devez utiliser le type d'algorithme composite. Si vous utilisez un algorithme `SHA-1` ou un algorithme de `SHA-256` somme de contrôle pour

le téléchargement d'une seule partie, seul le type d'algorithme d'objet complet est pris en charge.

Chargements en une seule partie

Les sommes de contrôle des objets chargés en une seule partie (à l'aide de `PutObject`) sont traitées comme des sommes de contrôle d'objets entiers. Lorsque vous chargez un objet dans la console Amazon S3, vous pouvez choisir l'algorithme de somme de contrôle que vous souhaitez que S3 utilise et, si vous le souhaitez, vous pouvez aussi fournir une valeur précalculée. Amazon S3 valide ensuite cette somme de contrôle avant de stocker l'objet et sa valeur de somme contrôle. Vous pouvez vérifier l'intégrité des données d'un objet lorsque vous demandez la valeur de la somme de contrôle lors du chargement de l'objet.

Chargements partitionnés

Lorsque vous chargez l'objet en plusieurs parties à l'aide de l'API `MultipartUpload`, vous pouvez spécifier l'algorithme de somme de contrôle que vous souhaitez qu'Amazon S3 utilise et le type de somme de contrôle (objet entier ou composite).

Le tableau suivant indique quel type d'algorithme de somme de contrôle est pris en charge pour chaque algorithme de somme de contrôle d'un chargement partitionné :

Algorithme de somme de contrôle	Objet complet	Composite
CRC-64/NVME () `CRC64NVME`	Oui	Non
CRC-32 () `CRC32`	Oui	Oui
CRC-32C () `CRC32C`	Oui	Oui
SHA-1 () `SHA1`	Non	Oui
SHA-256 () `SHA256`	Non	Oui

Utilisation des sommes de contrôle des objets entiers pour le chargement partitionné

Lorsque vous créez ou effectuez un chargement partitionné, vous pouvez utiliser les sommes de contrôle de l'objet entier pour la validation du chargement. Cela signifie que vous pouvez fournir l'algorithme de somme de contrôle pour l'API `MultipartUpload`, ce qui simplifie les outils de validation de l'intégrité, car vous n'avez plus besoin de suivre les limites de chaque partie pour les objets chargés. Vous pouvez fournir la somme de contrôle de l'objet entier dans la demande `CompleteMultipartUpload`, ainsi que la taille de l'objet.

Lorsque vous fournissez une somme de contrôle complète d'un objet lors d'un chargement en plusieurs parties, le AWS SDK transmet la somme de contrôle à Amazon S3, et S3 valide l'intégrité de l'objet côté serveur, en la comparant à la valeur reçue. Amazon S3 stocke ensuite l'objet si les valeurs correspondent. Si les deux valeurs ne correspondent pas, S3 fait échouer la demande et génère une erreur `BadDigest`. La somme de contrôle de votre objet est également stockée dans les métadonnées de l'objet que vous utiliserez ultérieurement pour valider l'intégrité des données d'un objet.

Pour les sommes de contrôle complètes des objets, vous pouvez utiliser les algorithmes de somme de contrôle CRC-64/NVME (`CRC64NVME`), CRC-32 (`CRC32`) ou CRC-32C () dans S3. `CRC32C` Les sommes de contrôle des objets entiers dans les chargements partitionnés ne sont disponibles que pour les sommes de contrôle basées sur l'algorithme CRC, car elles peuvent être linéarisées en une somme de contrôle pour l'objet entier. Cette linéarisation permet à Amazon S3 de paralléliser vos demandes pour améliorer les performances. S3 peut notamment calculer la somme de contrôle de l'objet entier à partir des sommes de contrôle au niveau de chaque partie. Ce type de validation n'est pas disponible pour les autres algorithmes, tels que SHA et MD5. Comme S3 dispose de protections d'intégrité par défaut, si des objets sont chargés sans somme de contrôle, S3 attache automatiquement l'algorithme de somme de contrôle CRC-64/NVME (`CRC64NVME`) recommandé pour l'ensemble de l'objet à l'objet.

> **Note**
>
> Pour lancer le chargement partitionné, vous pouvez spécifier l'algorithme de somme de contrôle et le type de somme de contrôle de l'objet entier. Après avoir spécifié l'algorithme de somme de contrôle et le type de somme de contrôle de l'objet entier, vous pouvez fournir la valeur de somme de contrôle de cet objet pour le chargement partitionné.

Utilisation des sommes de contrôle au niveau des parties d'un chargement partitionné

Lorsque des objets sont chargés sur Amazon S3, ils peuvent être chargés en tant qu'objet unique ou en plusieurs parties par le biais du processus de chargement partitionné. Vous pouvez choisir un type de somme de contrôle pour votre chargement partitionné. Pour les sommes de contrôle au niveau de chaque partie d'un chargement partitionné (ou les sommes de contrôle composites), Amazon S3 calcule la somme de contrôle pour chaque partie en utilisant l'algorithme de somme de contrôle spécifié. Vous pouvez utiliser `UploadPart` pour fournir les valeurs de somme de contrôle pour chaque partie. Si l'objet que vous essayez de télécharger dans la console Amazon S3 est configuré pour utiliser l'algorithme de somme de contrôle CRC-64/NVME (`CRC64NVME`) et dépasse 16 Mo, il est automatiquement désigné comme somme de contrôle d'objet complète.

Amazon S3 utilise ensuite les valeurs de somme de contrôle stockées au niveau de chaque partie pour confirmer que chacune d'elle est correctement chargée. Lorsque la somme de contrôle de chaque partie (de l'objet entier) est fournie, S3 utilise les valeurs de la somme de contrôle stockées pour chaque partie afin de calculer la somme de contrôle de l'objet entier en interne, en la comparant à la valeur de la somme de contrôle fournie. Les coûts de calcul sont ainsi réduits, car S3 peut calculer une somme de contrôle de l'objet entier en utilisant la somme de contrôle de chaque partie. Pour en savoir plus sur les chargements partitionnés, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3 et Utilisation des sommes de contrôle des objets entiers pour le chargement partitionné.

Lorsque l'objet est complètement chargé, vous pouvez utiliser la somme de contrôle finale calculée pour vérifier l'intégrité des données de l'objet.

Lors du chargement d'une partie du chargement partitionné, tenez compte des points suivants :

- Pour extraire des informations sur l'objet, notamment le nombre de parties qui le composent, vous pouvez utiliser l'opération `GetObjectAttributes`. Avec les sommes de contrôle supplémentaires, vous pouvez également récupérer des informations pour chaque partie individuelle, y compris la valeur de la somme de contrôle de chaque partie.
- Pour les chargements finalisés, vous pouvez obtenir la somme de contrôle d'une partie individuelle à l'aide des opérations `GetObject` ou `HeadObject` et en spécifiant un numéro de partie ou une plage d'octets qui correspond à sur une seule partie. Pour récupérer les valeurs de somme de contrôle de chaque partie des chargements partitionnés qui sont toujours en cours, vous pouvez utiliser `ListParts`.

- En raison de la façon dont Amazon S3 calcule le total de contrôle pour les objets à plusieurs parties, la valeur du total de contrôle de l'objet peut changer si vous le copiez. Si vous utilisez un kit SDK ou l'API REST et que vous appelez `CopyObject`, Amazon S3 copie tout objet conformément aux limites de taille de l'opération API `CopyObject`. Amazon S3 effectue cette copie en une seule action, que l'objet ait été chargé en une seule requête ou dans le cadre d'un chargement partitionné. Avec une commande de copie, le total de contrôle de l'objet est un total de contrôle direct de l'objet complet. Si l'objet a été initialement chargé à l'aide d'un chargement partitionné, la valeur de la somme de contrôle change même si les données ne changent pas.
- Les objets dont la taille dépasse les limites de l'opération d'API `CopyObject` doivent utiliser des commandes de copie par chargement partitionné.
- Lorsque vous effectuez certaines opérations à l'aide du AWS Management Console, Amazon S3 utilise un téléchargement partitionné si la taille de l'objet est supérieure à 16 Mo.

Opérations de somme de contrôle

Après avoir chargé des objets, vous pouvez obtenir la valeur de la somme de contrôle et la comparer à une valeur de somme de contrôle précalculée ou précédemment stockée pour le même type d'algorithme. Les exemples suivants illustrent les opérations ou méthodes de somme de contrôle vous pouvez utiliser pour vérifier l'intégrité des données.

Utilisation de la console S3

Pour en savoir plus sur l'utilisation de la console et la définition des algorithmes de somme de contrôle à utiliser lors du chargement d'objets, consultez Chargement d'objets et Didacticiel : Vérification de l'intégrité des données dans Amazon S3 avec des sommes de contrôle supplémentaires.

À l'aide du AWS SDKs

L'exemple suivant montre comment vous pouvez utiliser le AWS SDKs pour télécharger un fichier volumineux avec un téléchargement en plusieurs parties, télécharger un fichier volumineux et valider un fichier de téléchargement en plusieurs parties, le tout en utilisant SHA-256 pour la validation des fichiers.

Java

Example Exemple : chargement, téléchargement et vérification d'un fichier volumineux avec SHA-256

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import software.amazon.awssdk.auth.credentials.AwsCredentials;
import software.amazon.awssdk.auth.credentials.AwsCredentialsProvider;
import software.amazon.awssdk.core.ResponseInputStream;
import software.amazon.awssdk.core.sync.RequestBody;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.AbortMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.ChecksumMode;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CompleteMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.CompletedMultipartUpload;
import software.amazon.awssdk.services.s3.model.CompletedPart;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadRequest;
import software.amazon.awssdk.services.s3.model.CreateMultipartUploadResponse;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesRequest;
import software.amazon.awssdk.services.s3.model.GetObjectAttributesResponse;
import software.amazon.awssdk.services.s3.model.GetObjectRequest;
import software.amazon.awssdk.services.s3.model.GetObjectResponse;
import software.amazon.awssdk.services.s3.model.GetObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.ObjectAttributes;
import software.amazon.awssdk.services.s3.model.PutObjectTaggingRequest;
import software.amazon.awssdk.services.s3.model.Tag;
import software.amazon.awssdk.services.s3.model.Tagging;
import software.amazon.awssdk.services.s3.model.UploadPartRequest;
import software.amazon.awssdk.services.s3.model.UploadPartResponse;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.nio.ByteBuffer;
import java.security.MessageDigest;
```

```
    import java.security.NoSuchAlgorithmException;
    import java.util.ArrayList;
    import java.util.Base64;
    import java.util.List;

    public class LargeObjectValidation {
        private static String FILE_NAME = "sample.file";
        private static String BUCKET = "sample-bucket";
        //Optional, if you want a method of storing the full multipart object
 checksum in S3.
        private static String CHECKSUM_TAG_KEYNAME = "fullObjectChecksum";
        //If you have existing full-object checksums that you need to validate
 against, you can do the full object validation on a sequential upload.
        private static String SHA256_FILE_BYTES = "htCM5g7ZNdoSw8bN/
mkgiAhXt5MFoVowVg+LE9aIQmI=";
        //Example Chunk Size - this must be greater than or equal to 5MB.
        private static int CHUNK_SIZE = 5 * 1024 * 1024;

        public static void main(String[] args) {
            S3Client s3Client = S3Client.builder()
                    .region(Region.US_EAST_1)
                    .credentialsProvider(new AwsCredentialsProvider() {
                        @Override
                        public AwsCredentials resolveCredentials() {
                            return new AwsCredentials() {
                                @Override
                                public String accessKeyId() {
                                    return Constants.ACCESS_KEY;
                                }

                                @Override
                                public String secretAccessKey() {
                                    return Constants.SECRET;
                                }
                            };
                        }
                    })
                    .build();
            uploadLargeFileBracketedByChecksum(s3Client);
            downloadLargeFileBracketedByChecksum(s3Client);
            validateExistingFileAgainstS3Checksum(s3Client);
        }

        public static void uploadLargeFileBracketedByChecksum(S3Client s3Client) {
```

```
            System.out.println("Starting uploading file validation");
            File file = new File(FILE_NAME);
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256 = MessageDigest.getInstance("SHA-256");
                CreateMultipartUploadRequest createMultipartUploadRequest =
CreateMultipartUploadRequest.builder()
                        .bucket(BUCKET)
                        .key(FILE_NAME)
                        .checksumAlgorithm(ChecksumAlgorithm.SHA256)
                        .build();
                CreateMultipartUploadResponse createdUpload =
s3Client.createMultipartUpload(createMultipartUploadRequest);
                List<CompletedPart> completedParts = new ArrayList<CompletedPart>();
                int partNumber = 1;
                byte[] buffer = new byte[CHUNK_SIZE];
                int read = in.read(buffer);
                while (read != -1) {
                    UploadPartRequest uploadPartRequest =
UploadPartRequest.builder()

.partNumber(partNumber).uploadId(createdUpload.uploadId()).key(FILE_NAME).bucket(BUCKET).ch
                    UploadPartResponse uploadedPart =
s3Client.uploadPart(uploadPartRequest,
RequestBody.fromByteBuffer(ByteBuffer.wrap(buffer, 0, read)));
                    CompletedPart part =
CompletedPart.builder().partNumber(partNumber).checksumSHA256(uploadedPart.checksumSHA256()
                    completedParts.add(part);
                    sha256.update(buffer, 0, read);
                    read = in.read(buffer);
                    partNumber++;
                }
                String fullObjectChecksum =
Base64.getEncoder().encodeToString(sha256.digest());
                if (!fullObjectChecksum.equals(SHA256_FILE_BYTES)) {
                    //Because the SHA256 is uploaded after the part is uploaded; the
upload is bracketed and the full object can be fully validated.

s3Client.abortMultipartUpload(AbortMultipartUploadRequest.builder().bucket(BUCKET).key(FILE
                    throw new IOException("Byte mismatch between stored checksum and
upload, do not proceed with upload and cleanup");
                }
                CompletedMultipartUpload completedMultipartUpload =
CompletedMultipartUpload.builder().parts(completedParts).build();
```

```
                CompleteMultipartUploadResponse completedUploadResponse =
s3Client.completeMultipartUpload(

CompleteMultipartUploadRequest.builder().bucket(BUCKET).key(FILE_NAME).uploadId(createdUplo
                Tag checksumTag =
Tag.builder().key(CHECKSUM_TAG_KEYNAME).value(fullObjectChecksum).build();
                //Optionally, if you need the full object checksum stored with the
file; you could add it as a tag after completion.

s3Client.putObjectTagging(PutObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).t
            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
            GetObjectAttributesResponse
                    objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
            System.out.println(objectAttributes.objectParts().parts());
            System.out.println(objectAttributes.checksum().checksumSHA256());
        }

        public static void downloadLargeFileBracketedByChecksum(S3Client s3Client) {
            System.out.println("Starting downloading file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            try (OutputStream out = new FileOutputStream(file)) {
                GetObjectAttributesResponse
                        objectAttributes =
s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                        .objectAttributes(ObjectAttributes.OBJECT_PARTS,
ObjectAttributes.CHECKSUM).build());
                //Optionally if you need the full object checksum, you can grab a
tag you added on the upload
                List<Tag> objectTags =
s3Client.getObjectTagging(GetObjectTaggingRequest.builder().bucket(BUCKET).key(FILE_NAME).b
                String fullObjectChecksum = null;
                for (Tag objectTag : objectTags) {
                    if (objectTag.key().equals(CHECKSUM_TAG_KEYNAME)) {
                        fullObjectChecksum = objectTag.value();
                        break;
                    }
                }
                MessageDigest sha256FullObject =
MessageDigest.getInstance("SHA-256");
```

```
                MessageDigest sha256ChecksumOfChecksums =
 MessageDigest.getInstance("SHA-256");

                //If you retrieve the object in parts, and set the ChecksumMode to
 enabled, the SDK will automatically validate the part checksum
                for (int partNumber = 1; partNumber <=
 objectAttributes.objectParts().totalPartsCount(); partNumber++) {
                    MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                    ResponseInputStream<GetObjectResponse> response =
 s3Client.getObject(GetObjectRequest.builder().bucket(BUCKET).key(FILE_NAME).partNumber(part
                    GetObjectResponse getObjectResponse = response.response();
                    byte[] buffer = new byte[CHUNK_SIZE];
                    int read = response.read(buffer);
                    while (read != -1) {
                        out.write(buffer, 0, read);
                        sha256FullObject.update(buffer, 0, read);
                        sha256Part.update(buffer, 0, read);
                        read = response.read(buffer);
                    }
                    byte[] sha256PartBytes = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(sha256PartBytes);
                    //Optionally, you can do an additional manual validation again
 the part checksum if needed in addition to the SDK check
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(sha256PartBytes);
                    String base64PartChecksumFromObjectAttributes =
 objectAttributes.objectParts().parts().get(partNumber - 1).checksumSHA256();
                    if (!
base64PartChecksum.equals(getObjectResponse.checksumSHA256()) || !
base64PartChecksum.equals(base64PartChecksumFromObjectAttributes)) {
                        throw new IOException("Part checksum didn't match for the
 part");
                    }
                    System.out.println(partNumber + " " + base64PartChecksum);
                }
                //Before finalizing, do the final checksum validation.
                String base64FullObject =
 Base64.getEncoder().encodeToString(sha256FullObject.digest());
                String base64ChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                if (fullObjectChecksum != null && !
fullObjectChecksum.equals(base64FullObject)) {
                    throw new IOException("Failed checksum validation for full
 object");
```

```
                }
                System.out.println(fullObjectChecksum);
                String base64ChecksumOfChecksumFromAttributes =
 objectAttributes.checksum().checksumSHA256();
                if (base64ChecksumOfChecksumFromAttributes != null && !
base64ChecksumOfChecksums.equals(base64ChecksumOfChecksumFromAttributes)) {
                    throw new IOException("Failed checksum validation for full
 object checksum of checksums");
                }
                System.out.println(base64ChecksumOfChecksumFromAttributes);
                out.flush();
            } catch (IOException | NoSuchAlgorithmException e) {
                //Cleanup bad file
                file.delete();
                e.printStackTrace();
            }
        }

        public static void validateExistingFileAgainstS3Checksum(S3Client s3Client)
 {
            System.out.println("Starting existing file validation");
            File file = new File("DOWNLOADED_" + FILE_NAME);
            GetObjectAttributesResponse
                    objectAttributes =
 s3Client.getObjectAttributes(GetObjectAttributesRequest.builder().bucket(BUCKET).key(FILE_N
                    .objectAttributes(ObjectAttributes.OBJECT_PARTS,
 ObjectAttributes.CHECKSUM).build());
            try (InputStream in = new FileInputStream(file)) {
                MessageDigest sha256ChecksumOfChecksums =
 MessageDigest.getInstance("SHA-256");
                MessageDigest sha256Part = MessageDigest.getInstance("SHA-256");
                byte[] buffer = new byte[CHUNK_SIZE];
                int currentPart = 0;
                int partBreak =
 objectAttributes.objectParts().parts().get(currentPart).size();
                int totalRead = 0;
                int read = in.read(buffer);
                while (read != -1) {
                    totalRead += read;
                    if (totalRead >= partBreak) {
                        int difference = totalRead - partBreak;
                        byte[] partChecksum;
                        if (totalRead != partBreak) {
                            sha256Part.update(buffer, 0, read - difference);
```

```
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
                            sha256Part.reset();
                            sha256Part.update(buffer, read - difference,
 difference);
                        } else {
                            sha256Part.update(buffer, 0, read);
                            partChecksum = sha256Part.digest();
                            sha256ChecksumOfChecksums.update(partChecksum);
                            sha256Part.reset();
                        }
                        String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                        if (!
base64PartChecksum.equals(objectAttributes.objectParts().parts().get(currentPart).checksumSH
 {
                            throw new IOException("Part checksum didn't match S3");
                        }
                        currentPart++;
                        System.out.println(currentPart + " " + base64PartChecksum);
                        if (currentPart <
 objectAttributes.objectParts().totalPartsCount()) {
                            partBreak +=
 objectAttributes.objectParts().parts().get(currentPart - 1).size();
                        }
                    } else {
                        sha256Part.update(buffer, 0, read);
                    }
                    read = in.read(buffer);
                }
                if (currentPart != objectAttributes.objectParts().totalPartsCount())
 {
                    currentPart++;
                    byte[] partChecksum = sha256Part.digest();
                    sha256ChecksumOfChecksums.update(partChecksum);
                    String base64PartChecksum =
 Base64.getEncoder().encodeToString(partChecksum);
                    System.out.println(currentPart + " " + base64PartChecksum);
                }

                String base64CalculatedChecksumOfChecksums =
 Base64.getEncoder().encodeToString(sha256ChecksumOfChecksums.digest());
                System.out.println(base64CalculatedChecksumOfChecksums);
                System.out.println(objectAttributes.checksum().checksumSHA256());
```

```
                if (!
base64CalculatedChecksumOfChecksums.equals(objectAttributes.checksum().checksumSHA256()))
 {
                    throw new IOException("Full object checksum of checksums don't
 match S3");
                }

            } catch (IOException | NoSuchAlgorithmException e) {
                e.printStackTrace();
            }
        }
    }
```

Utilisation de l'API REST

Vous pouvez envoyer des requêtes REST pour télécharger un objet avec une valeur de somme de contrôle afin de vérifier l'intégrité des PutObjectdonnées. Vous pouvez également récupérer la valeur de la somme de contrôle pour les objets à l'aide de GetObjectou HeadObject.

À l'aide du AWS CLI

Vous pouvez envoyer une demande PUT pour télécharger un objet d'une taille maximale de 5 Go en une seule opération. Pour plus d'informations, reportez-vous à la section `PutObject` dans la Référence des commandes de l'AWS CLI . Vous pouvez également utiliser `get-object` et `head-object` pour récupérer le total de contrôle d'un objet déjà chargé afin de vérifier l'intégrité des données.

Pour plus d'informations, consultez la FAQ de l'interface de ligne de commande Amazon S3 dans le Guide de l'utilisateur AWS Command Line Interface .

Utilisation de Content- MD5 lors du téléchargement d'objets

Une autre façon de vérifier l'intégrité de votre objet après le téléchargement consiste à fournir un MD5 résumé de l'objet lorsque vous le chargez. Si vous calculez le MD5 résumé de votre objet, vous pouvez le fournir avec la PUT commande en utilisant l'`Content-MD5`en-tête.

Après avoir chargé l'objet, Amazon S3 calcule le MD5 résumé de l'objet et le compare à la valeur que vous avez fournie. La requête n'aboutit que si les deux récapitulatifs correspondent.

Il n'est pas nécessaire de fournir un MD5 résumé, mais vous pouvez l'utiliser pour vérifier l'intégrité de l'objet dans le cadre du processus de téléchargement.

Utilisation du contenu MD5 et du ETag pour vérifier les objets téléchargés

La balise d'entité (ETag) d'un objet représente une version spécifique de cet objet. N'oubliez pas que cela reflète ETag uniquement les modifications apportées au contenu d'un objet, et non les modifications apportées à ses métadonnées. Si seules les métadonnées d'un objet changent, elles ETag restent les mêmes.

Selon l'objet, ETag l'objet peut être un MD5 condensé des données de l'objet :

- Si un objet est créé par l'`CopyObject`opération `PutObject``PostObject`, ou par le biais de AWS Management Console, et que cet objet est également en texte brut ou chiffré par chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3), cet objet possède un ETag MD5 condensé de ses données d'objet.
- Si un objet est créé par l'`CopyObject`opération `PutObject``PostObject`, ou par le biais de AWS Management Console, et que cet objet est chiffré par chiffrement côté serveur avec des clés fournies par le client (SSE-C) ou par chiffrement côté serveur avec des clés () (SSE-KMS AWS KMS), cet objet possède un code qui n'est pas un ETag condensé de ses données d'objet. AWS Key Management Service MD5
- Si un objet est créé soit par le processus de téléchargement en plusieurs parties, soit par l'`UploadPartCopy`opération, il ne ETag s'agit pas d'un MD5 condensé, quelle que soit la méthode de chiffrement utilisée. Si la taille d'un objet est supérieure à 16 Mo, il AWS Management Console télécharge ou copie cet objet sous forme de téléchargement partitionné ; il ne s'agit donc ETag pas d'un MD5 résumé.

Pour les objets dont le résumé ETag est le `Content-MD5` condensé de l'objet, vous pouvez comparer la ETag valeur de l'objet avec un `Content-MD5` résumé calculé ou enregistré précédemment.

Utilisation des totaux de contrôle de fin

Lorsque vous chargez des objets sur Amazon S3, vous pouvez soit fournir une somme de contrôle précalculée pour l'objet, soit utiliser un AWS SDK pour créer automatiquement des sommes de contrôle de suivi pour les téléchargements fragmentés, en votre nom. Si vous utilisez une somme de contrôle finale, Amazon S3 génère automatiquement la somme de contrôle en utilisant l'algorithme que vous avez spécifié pour valider l'intégrité de l'objet dans les téléchargements fragmentés, lorsque vous chargez un objet.

Pour créer une somme de contrôle finale lors de l'utilisation d'un AWS SDK, renseignez le `ChecksumAlgorithm` paramètre avec votre algorithme préféré. Le SDK utilise cet algorithme pour calculer la somme de contrôle pour votre objet (ou des parties de l'objet) et l'ajoute automatiquement à la fin de votre demande de téléchargement segmentée. Ce comportement vous fait gagner du temps car Amazon S3 effectue la vérification et le chargement de vos données en une seule opération.

> **Important**
>
> Si vous utilisez S3 Object Lambda, toutes les requêtes adressées à S3 Object Lambda sont signées en utilisant `s3-object-lambda` au lieu de `s3`. Ce comportement affecte la signature des valeurs de total de contrôle de fin. Pour en savoir plus sur S3 Object Lambda, consultez Transformation d'objets avec S3 Object Lambda.

En-têtes de somme de contrôle suivants

Pour effectuer une demande de codage de contenu fragmenté, Amazon S3 demande aux clients d'inclure plusieurs en-têtes afin d'analyser correctement la demande. Les clients doivent inclure les en-têtes suivants :

- **`x-amz-decoded-content-length`**: Cet en-tête indique la taille du texte brut des données réelles qui sont chargées sur Amazon S3 avec la demande.
- **`x-amz-content-sha256`**: Cet en-tête indique le type de téléchargement fragmenté inclus dans la demande. Pour les téléchargements fragmentés avec des sommes de contrôle finales, la valeur d'en-tête est `STREAMING-UNSIGNED-PAYLOAD-TRAILER` destinée aux demandes qui n'utilisent pas la signature de charge utile et aux demandes qui utilisent la signature de charge utile `STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER` SigV4. (Pour plus d'informations sur l'implémentation de charges utiles signées, voir Calculs de signature pour l'en-tête d'autorisation : transfert d'une charge utile en plusieurs segments.)
- **`x-amz-trailer`**: Cet en-tête indique le nom de l'en-tête final de la demande. S'il existe des sommes de contrôle finales (AWS SDKs ajoutez des sommes de contrôle aux corps de demande codés), la valeur d'`x-amz-trailer`en-tête inclut le `x-amz-checksum-` préfixe et se termine par le nom de l'algorithme. Les `x-amz-trailer` valeurs suivantes sont actuellement prises en charge :
  - `x-amz-checksum-crc32`
  - `x-amz-checksum-crc32c`

- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha256`

> **Note**
>
> Vous pouvez également inclure l'`Content-Encoding`en-tête, avec la valeur segmentée, dans votre demande. Bien que cet en-tête ne soit pas obligatoire, son inclusion peut minimiser les problèmes de proxy HTTP lors de la transmission de données codées. Si un autre `Content-Encoding` en-tête (tel que gzip) existe dans la demande, l'`Content-Encoding`en-tête inclut la valeur segmentée dans une liste d'encodages séparés par des virgules. Par exemple, `Content-Encoding: aws-chunked, gzip`.

Pièces fragmentées

Lorsque vous chargez un objet sur Amazon S3 à l'aide d'un codage fragmenté, la demande de téléchargement inclut les types de fragments suivants (formatés dans l'ordre indiqué) :

- Morceaux de corps d'objet : il peut y avoir un, plusieurs ou aucun fragment de corps associé à une demande de téléchargement fragmenté.
- Morceaux d'achèvement : il peut y avoir un, plusieurs ou aucun segment de corps associé à une demande de téléchargement fragmenté.
- Morceaux de fin : La somme de contrôle de fin est répertoriée après le segment de fin. Un seul morceau final est autorisé.

> **Note**
>
> Chaque téléchargement fragmenté doit se terminer par un CRLF final (tel que`\r\n`) pour indiquer la fin de la demande.

Pour des exemples de mise en forme fragmentée, consultezExemples : téléchargements fragmentés avec des sommes de contrôle.

Morceaux du corps de l'objet

Les fragments du corps de l'objet sont les fragments qui contiennent les données d'objet réelles qui sont téléchargées vers S3. Ces morceaux sont soumis à des contraintes de taille et de format cohérentes.

Taille du morceau du corps de l'objet

Ces fragments doivent contenir au moins 8 192 octets (ou 8 KiB) de données d'objet, à l'exception du dernier segment du corps, qui peut être plus petit. Il n'y a pas de taille maximale explicite, mais vous pouvez vous attendre à ce que tous les morceaux soient inférieurs à la taille de téléchargement maximale de 5 Go. La taille des fragments peut varier d'un morceau à l'autre en fonction de l'implémentation de votre serveur client.

Format de bloc du corps de l'objet

Les fragments de corps d'objet commencent par le codage hexadécimal du nombre d'octets qu'ils contiennent, suivi d'un CRLF (Carriage Return Line Feed), des octets de l'objet correspondant à ce segment et d'un autre CRLF.

Par exemple :

```
hex-encoding-of-object-bytes-in-chunk\r\n
chunk-object-bytes\r\n
```

Toutefois, lorsque le fragment est signé, le segment du corps de l'objet suit un format différent, dans lequel la signature est ajoutée à la taille du bloc par un point-virgule. Par exemple :

```
hex-encoding-of-object-bytes-in-chunk;chunk-signature\r\n
 chunk-object-bytes\r\n
```

Pour plus d'informations sur la signature par morceaux, voir Calculs de signature pour l'Authorizationen-tête : transfert d'une charge utile en plusieurs fragments (AWS Signature version 4). Pour plus d'informations sur le formatage des blocs, consultez la section Codage de transfert par blocs sur le site Web de l'éditeur RFC.

Morceaux de complétion

Les fragments d'achèvement doivent être le dernier fragment du corps de l'objet de chaque téléchargement fragmenté. Le format d'un segment de complétion est similaire à celui d'un bloc de

corps, mais il ne contient toujours aucun octet de données d'objet. (Le zéro octet de données d'objet indique que toutes les données ont été téléchargées.) Les téléchargements fragmentés doivent inclure un fragment d'achèvement comme dernier fragment du corps de l'objet, selon un format comme celui-ci :

```
0\r\n
```

Toutefois, si la demande de codage de contenu utilise la signature de charge utile, elle suit plutôt le format suivant :

```
0;chunk-signature\r\n
```

Morceaux de remorque

Les segments de bande-annonce contiennent la somme de contrôle calculée pour toutes les demandes de téléchargement S3. Les segments de bande-annonce incluent deux champs : un champ de nom d'en-tête et un champ de valeur d'en-tête. Le champ du nom d'en-tête d'une demande de téléchargement doit correspondre à la valeur transmise dans l'en-tête de la `x-amz-trailer` demande. Par exemple, si une demande contient le nom `x-amz-trailer: x-amz-checksum-crc32` d'en-tête du fragment de la bande-annonce`x-amz-checksum-sha1`, la demande échoue. Le champ de valeur du fragment de bande-annonce inclut un codage base64 de la valeur de la somme de contrôle big-endian pour cet objet. (L'ordre big-endian stocke l'octet de données le plus significatif à l'adresse mémoire la plus basse et l'octet le moins significatif à la plus grande adresse mémoire). L'algorithme utilisé pour calculer cette somme de contrôle est le même que le suffixe du nom d'en-tête (par exemple,`crc32`).

Format des morceaux de la bande-annonce

Les segments de remorque utilisent le format suivant pour les demandes de charge utile non signées :

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\n\r\n\r\n
```

Pour les demandes contenant des charges utiles signées SigV4, le fragment de remorque inclut une signature de remorque après le morceau de remorque.

```
trailer-checksum\n\r\n
```

```
trailer-signature\r\n
```

Vous pouvez également ajouter le CRLF directement à la fin de la valeur de la somme de contrôle base64. Par exemple :

```
x-amz-checksum-lowercase-checksum-algorithm-name:base64-checksum-value\r\n\r\n
```

Exemples : téléchargements fragmentés avec des sommes de contrôle

Amazon S3 prend en charge les téléchargements fragmentés qui utilisent le codage `aws-chunked` du contenu `PutObject` et les `UploadPart` demandes avec des sommes de contrôle ultérieures.

Example 1 — **`PutObject`** Demande fragmentée non signée avec une somme de contrôle CRC-32

Voici un exemple de `PutObject` demande segmentée avec une somme de contrôle CRC-32 à la fin. Dans cet exemple, le client télécharge un objet de 17 Ko en trois segments non signés et ajoute un bloc de somme de contrôle CRC-32 final en utilisant l'en-tête. `x-amz-checksum-crc32`

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-UNSIGNED-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

2000\r\n                                    // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000\r\n                                    // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400\r\n                                     // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0\r\n                                       // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n\r\n     // Trailer chunk (note optional \n
 character)
\r\n                                          // CRLF
```

Voici un exemple de réponse :

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

> **Note**
>
> L'utilisation du fil \n à la fin de la valeur de la somme de contrôle peut varier d'un client à l'autre.

Example 2 — **`PutObject`** Demande fragmentée signée SIGv4 avec une somme de contrôle CRC-32 () à la fin **`CRC32`**

Voici un exemple de `PutObject` demande segmentée avec une somme de contrôle CRC-32 à la fin. Cette demande utilise la signature de la charge utile SigV4. Dans cet exemple, le client télécharge un objet de 17 Ko en trois parties signées. En plus des `object body` morceaux, les `completion chunk` et `trailer chunk` sont également signés.

```
PUT /Key+ HTTP/1.1
Host: amzn-s3-demo-bucket.s3.amazonaws.com
Content-Encoding: aws-chunked
x-amz-decoded-content-length: 17408
x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD-TRAILER
x-amz-trailer: x-amz-checksum-crc32

authorization-code                              // SigV4 headers authorization

2000;chunk-signature=signature-value...\r\n   // Object body chunk 1 (8192 bytes)
object-bytes\r\n
2000;chunk-signature\r\n                        // Object body chunk 2 (8192 bytes)
object-bytes\r\n
400;chunk-signature\r\n                         // Object body chunk 3 (1024 bytes)
object-bytes\r\n
0;chunk-signature\r\n                           // Completion chunk
x-amz-checksum-crc32:YABb/g==\n\r\n             // Trailer chunk (note optional \n
 character)
trailer-signature\r\n
\r\n                                            // CRLF
```

Voici un exemple de réponse :

```
HTTP/1.1 200
ETag: ETag
x-amz-checksum-crc32: YABb/g==
```

Suppression d'objets Amazon S3

Vous pouvez supprimer un ou plusieurs objets directement depuis Amazon S3 à l'aide de la console Amazon S3 AWS SDKs, AWS Command Line Interface (AWS CLI) ou de l'API REST. Par exemple, si vous collectez des fichiers journaux, vous pouvez les supprimer lorsque vous n'en avez plus besoin. Vous pouvez configurer une règle de cycle de vie S3 pour supprimer automatiquement les objets tels que les fichiers journaux.

Pour supprimer un objet, vous pouvez utiliser l'une des opérations d'API suivantes :

- Supprimer un seul objet : Amazon S3 fournit l'opération d'API `DELETE` (`DeleteObject`) que vous pouvez utiliser pour supprimer un objet en une seule demande HTTP.
- Supprimer plusieurs objets : Amazon S3 fournit l'opération d'API de suppression de plusieurs objets (`DeleteObjects`) que vous pouvez utiliser pour supprimer jusqu'à 1 000 objets en une seule demande HTTP.

Lorsque vous supprimez des objets d'un compartiment pour lequel la gestion des versions n'est pas activée, vous ne fournissez que le nom de la clé d'objet. Toutefois, lorsque vous supprimez des objets d'un compartiment pour lequel la gestion des versions est activée, vous pouvez fournir l'ID de version de l'objet pour supprimer cette version spécifique de l'objet.

Bonnes pratiques à prendre en compte avant de supprimer un objet

Avant de supprimer un objet, tenez compte des bonnes pratiques ci-dessous :

- Activez la gestion des versions dans le compartiment. La gestion des versions S3 renforce la protection contre les demandes `DeleteObject` simples afin d'éviter les suppressions accidentelles. Pour les compartiments pour lesquels la gestion des versions est activée, si vous supprimez la version actuelle d'un objet ou lorsqu'une demande de suppression ne spécifie pas d'identifiant de version spécifique, Amazon S3 ne supprime pas définitivement l'objet. Au lieu de cela, S3 ajoute un marqueur de suppression, qui génère une suppression progressive de l'objet. Le marqueur de suppression devient alors la version actuelle (ou la plus récente) de l'objet avec un nouvel ID de version. Pour plus d'informations, consultez Suppression des versions d'objet d'un compartiment activé pour la gestion des versions.
- Si vous souhaitez supprimer un grand nombre d'objets ou supprimer des objets par programmation en fonction de leur date de création, définissez une configuration de cycle de vie S3 au niveau du compartiment. Pour contrôler ces suppressions, nous vous recommandons d'utiliser une

notification d'événement de cycle de vie S3. Lorsque vous configurez les notifications de cycle de vie S3, le type d'événement `s3:LifecycleExpiration:Delete` vous avertit lorsqu'un objet d'un compartiment est supprimé. Il vous avertit également lorsqu'une version d'objet est définitivement supprimée par une configuration de cycle de vie S3. Le type d'événement `s3:LifecycleExpiration:DeleteMarkerCreated` vous avertit lorsque le cycle de vie S3 crée un marqueur de suppression. Un marqueur de suppression est créé lors de la suppression d'une version actuelle d'un objet dans un compartiment pour lequel la gestion des versions est activée.

- Avant de mettre à jour votre configuration de cycle de vie S3, vérifiez que le cycle de vie a mené à bien les actions sur tous les objets prévus. Pour plus d'informations, consultez la section Mise à jour, désactivation ou suppression des règles de cycle de vie dans Configuration d'une configuration du cycle de vie S3 sur un compartiment.

  > **Note**
  >
  > Les règles de cycle de vie S3 doivent s'appliquer au sous-ensemble d'objets approprié afin d'éviter les suppressions involontaires. Vous pouvez filtrer les objets par préfixes, balises d'objet ou tailles d'objet lors de la création des règles de cycle de vie.

- Envisagez d'empêcher les utilisateurs de retirer ou de supprimer des objets de votre compartiment. Pour restreindre les utilisateurs, vous devez explicitement leur refuser les autorisations pour les actions suivantes dans le cadre de vos politiques de compartiment Amazon S3 :
  - `s3:DeleteObject`, `s3:DeleteObjectVersion` (pour contrôler qui peut supprimer des objets à l'aide de requêtes d'API)
  - `s3:PutLifecycleConfiguration` (pour contrôler qui peut ajouter des règles d'expiration du cycle de vie S3)
- Envisagez d'utiliser la réplication S3 pour créer plusieurs copies de vos données et les répliquer simultanément sur plusieurs sites. Vous pouvez choisir autant de compartiments de destination que vous le souhaitez. De plus, si un objet est supprimé par inadvertance, vous aurez toujours une copie des données.

Suppression d'objets à partir d'un compartiment avec gestion des versions activée

Si la gestion des versions est activée pour votre compartiment, plusieurs versions du même objet peuvent coexister dans ce compartiment. Si vous utilisez des compartiments pour lesquels la gestion des versions a été activée, les opérations d'API `Delete` permettent les options suivantes :

- Spécifier une demande de suppression sans la gestion des versions : spécifiez uniquement la clé de l'objet, et non l'ID de la version. Dans ce cas, Amazon S3 crée un marqueur de suppression sur la version actuelle de l'objet et renvoie son ID de version dans la réponse. Votre objet n'apparaît plus dans le compartiment. Pour plus d'informations sur la gestion des versions d'objets et le concept des marqueurs de suppression, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.
- Spécifier une demande de suppression avec la gestion des versions : spécifiez à la fois la clé et l'ID de version. Dans ce cas, les résultats suivants sont possibles :
  - Si l'ID de version est lié à une version d'objet spécifique, Amazon S3 supprime la version spécifique de l'objet.
  - Si l'ID de version est lié au marqueur de suppression d'un objet, Amazon S3 supprime le marqueur de suppression. Lorsque le marqueur de suppression est supprimé, l'objet réapparaît dans le compartiment.

Suppression d'objets à partir d'um compartiment avec gestion des versions désactivée

Si la gestion des versions est suspendue au niveau du compartiment, les opérations d'API `Delete` se comportent de la même manière pour les compartiments pour lesquels la gestion des versions est activée (sauf lorsque la version actuelle possède un ID de version nul). Pour de plus amples informations, veuillez consulter Suppression d'objets à partir des compartiments désactivés pour la gestion des versions.

Suppression d'objets à partir d'un compartiment sans gestion des versions

Si la gestion des versions n'est pas activée pour votre compartiment, vous pouvez spécifier la clé de l'objet dans les opérations d'API `Delete` pour qu'Amazon S3 supprime définitivement l'objet. Pour empêcher la suppression définitive d'un objet, activez la gestion des versions au niveau des compartiments.

Suppression des objets d'un compartiment avec authentification MFA activée

Lorsque vous supprimez des objets d'un compartiment prenant en charge l'authentification multifacteur (MFA), notez les points suivants :

- Si vous fournissez un jeton d'authentification MFA non valide, la demande échouera.
- Si vous avez un compartiment activé pour l'authentification MFA et que vous faites une demande de suppression avec la gestion de version (vous fournissez une clé d'objet et un ID de version), la demande échoue si vous ne fournissez pas un jeton d'authentification MFA valide. En outre, avec l'opération d'API `Delete` supprimant plusieurs objets dans un compartiment pour lequel l'authentification MFA est activée, si l'un des objets supprimés est une demande de suppression avec la gestion des versions (à savoir, si vous indiquez la clé de l'objet et l'ID de version), la demande échouera dans son intégralité si vous ne fournissez aucun jeton d'authentification MFA.

Toutefois, dans les cas suivants, la demande réussit :

- Si vous avez un compartiment pour lequel l'authentification MFA est activée et que vous faites une demande de suppression sans la gestion des versions (vous ne supprimez pas un objet avec la gestion des versions), et que vous ne fournissez pas de jeton d'authentification MFA, la suppression aboutit.
- Si vous avez une demande de suppression de plusieurs objets spécifiant des objets sans la gestion des versions à supprimer d'un compartiment pour lequel l'authentification MFA est activée, et que vous ne fournissez pas de jeton d'authentification MFA, la suppression aboutit.

Pour en savoir plus sur la suppression MFA, consultez Configuration de la fonction Supprimer MFA.

Rubriques

- Suppression d'un seul objet
- Suppression de plusieurs objets

Suppression d'un seul objet

Vous pouvez utiliser la console Amazon S3 ou l'API DELETE pour supprimer un seul objet existant d'un compartiment S3. Pour plus d'informations sur la suppression d'objets dans Amazon S3, consultez Suppression d'objets Amazon S3.

Etant donné que tous les objets dans le compartiment S3 entraînent des coûts de stockage, vous devez supprimer ceux dont vous n'avez plus besoin. Par exemple, si vous collectez des fichiers journaux, vous pouvez les supprimer lorsque vous n'en avez plus besoin. Vous pouvez configurer une règle de cycle de vie pour supprimer automatiquement les objets tels que les fichiers journaux. Pour plus d'informations, consultez the section called "Définition d'une configuration de cycle de vie".

Pour en savoir plus sur les fonctions et la tarification d'Amazon S3, veuillez consulter Tarification Amazon S3.

Utiliser la console S3.

Procédez comme suit pour utiliser la console Amazon S3 pour supprimer un seul objet d'un compartiment.

> **Warning**
>
> Lorsque vous supprimez définitivement un objet ou une version d'objet spécifiée dans la console Amazon S3, cette opération est irréversible.

Pour supprimer un objet pour lequel la gestion des versions est activée ou suspendue

> **Note**
>
> Si l'ID de version d'un objet dans un compartiment pour lequel la gestion des versions est suspendue, est marqué comme NULL, S3 supprime définitivement l'objet, car il n'existe aucune version précédente. Toutefois, si un ID de version valide est répertorié pour l'objet dans un compartiment pour lequel la gestion des versions est suspendue, S3 crée un marqueur de suppression pour l'objet supprimé, tout en conservant les versions précédentes de l'objet.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment dont vous souhaitez supprimer un objet.

4. Sélectionnez l'objet, puis choisissez Supprimer.
5. Pour confirmer la suppression de la liste d'objets sous Objets spécifiés dans la zone de texte Supprimer les objets ?, entrez **`delete`**.

Pour supprimer une version d'objet spécifique dans un compartiment pour lequel la gestion des versions est activée

> **Warning**
>
> Lorsque vous supprimez définitivement une version d'objet spécifique dans Amazon S3, cette opération est irréversible.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment à partir duquel vous souhaitez supprimer un objet.
3. Sélectionnez l'objets que vous voulez supprimer.
4. Choisissez le bouton Afficher les versions.
5. Sélectionnez la version de l'objet, puis choisissez Supprimer.
6. Pour confirmer la suppression définitive des versions d'objets spécifiques répertoriées sous Objets spécifiés, dans la zone de texte Supprimer les objets ?, entrez Supprimer définitivement. Amazon S3 supprime définitivement cette version spécifique de l'objet.

Pour supprimer définitivement un objet dans un compartiment Amazon S3 pour lequel la gestion des versions n'est pas activée

> **Warning**
>
> Lorsque vous supprimez définitivement un objet dans Amazon S3, cette opération est irréversible. De plus, pour tous les compartiments pour lesquels la gestion des versions n'est pas activée, les suppressions sont permanentes.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment dont vous souhaitez supprimer un objet.
4. Sélectionnez l'objet, puis choisissez Supprimer.
5. Pour confirmer la suppression définitive de l'objet répertorié sous Objets spécifiés, dans la zone de texte Supprimer des objets ?, entrez Supprimer définitivement.

> **Note**
>
> Si vous rencontrez des problèmes lors de la suppression de l'objet, consultez Je souhaite supprimer définitivement les objets avec la gestion des versions.

À l'aide du AWS CLI

Pour supprimer un objet par demande, utilisez l'API `DELETE`. Pour plus d'informations, consultez Objet DELETE. Pour plus d'informations sur l'utilisation de la CLI pour supprimer un objet, consultez delete-object.

Utilisation de l'API REST

Vous pouvez utiliser le AWS SDKs pour supprimer un objet. Toutefois, si l'application l'exige, vous pouvez envoyer directement des demandes REST. Pour plus d'informations, consultez Objet DELETE dans la Référence d'API Amazon Simple Storage Service.

À l'aide du AWS SDKs

Les exemples suivants montrent comment vous pouvez utiliser le AWS SDKs pour supprimer un objet d'un compartiment. Pour plus d'informations, consultez Objet DELETE dans la Référence d'API Amazon Simple Storage Service.

Si le compartiment est activé pour la gestion des versions S3, vous disposez des options suivantes :

- Supprimez une version spécifique d'objet en spécifiant un ID de version.
- Supprimez un objet sans spécifier un ID de version, auquel cas Amazon S3 ajoute un marqueur de suppression à l'objet.

Pour plus d'informations sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Pour plus d'exemples, et des exemples dans d'autres langages, consultez Utiliser `DeleteObject` avec un AWS SDK ou une CLI dans le manuel de référence de l'API Amazon S3.

Java

Example Exemple 1 : Suppression d'un objet (compartiment désactivé pour la gestion des versions)

L'exemple suivant suppose que le bucket n'est pas activé pour la gestion des versions et que l'objet n'a aucune version. IDs Dans la demande de suppression, vous ne spécifiez que la clé d'objet, et pas d'ID de version.

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

import java.io.IOException;

public class DeleteObjectNonVersionedBucket {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            s3Client.deleteObject(new DeleteObjectRequest(bucketName, keyName));
```

```
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example Exemple 2 : Suppression d'un objet (compartiment activé pour la gestion des versions)

L'exemple suivant supprime un objet à partir d'un compartiment activé pour la gestion des versions. L'exemple supprime une version d'objet spécifique en spécifiant le nom de la clé d'objet et l'ID de version.

Cet exemple effectue les opérations suivantes :

1. Ajoute un exemple d'objet au compartiment. Amazon S3 renvoie l'ID de version de l'objet nouvellement ajouté. L'exemple utilise l'ID de version dans la demande de suppression.
2. Supprime la version d'objet spécifique en spécifiant le nom de la clé d'objet et l'ID de version. S'il n'existe pas d'autres versions de cet objet, Amazon S3 supprime la totalité de l'objet. Sinon, Amazon S3 supprime uniquement la version spécifiée.

> **Note**
>
> Vous pouvez obtenir la version IDs d'un objet en envoyant une `ListVersions` demande.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
```

```
import com.amazonaws.services.s3.model.DeleteVersionRequest;
import com.amazonaws.services.s3.model.PutObjectResult;

import java.io.IOException;

public class DeleteObjectVersionEnabledBucket {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ****";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Check to ensure that the bucket is versioning-enabled.
            String bucketVersionStatus =
 s3Client.getBucketVersioningConfiguration(bucketName).getStatus();
            if (!bucketVersionStatus.equals(BucketVersioningConfiguration.ENABLED))
 {
                System.out.printf("Bucket %s is not versioning-enabled.",
 bucketName);
            } else {
                // Add an object.
                PutObjectResult putResult = s3Client.putObject(bucketName, keyName,
                        "Sample content for deletion example.");
                System.out.printf("Object %s added to bucket %s\n", keyName,
 bucketName);

                // Delete the version of the object that we just created.
                System.out.println("Deleting versioned object " + keyName);
                s3Client.deleteVersion(new DeleteVersionRequest(bucketName, keyName,
 putResult.getVersionId()));
                System.out.printf("Object %s, version %s deleted\n", keyName,
 putResult.getVersionId());
            }
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
```

```
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Les exemples suivants montrent comment supprimer un objet à partir d'un compartiment activé pour la gestion des versions et d'un compartiment non activé pour la gestion des versions. Pour plus d'informations sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Example Suppression d'un objet d'un compartiment désactivé pour la gestion des versions

L'exemple C# suivant supprime un objet à partir d'un compartiment désactivé pour la gestion des versions. L'exemple suppose que les objets n'ont pas de version IDs, vous ne spécifiez donc pas de version IDs. Spécifiez uniquement la clé d'objet.

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectNonVersionedBucketTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
```

```
        {
            client = new AmazonS3Client(bucketRegion);
            DeleteObjectNonVersionedBucketAsync().Wait();
        }
        private static async Task DeleteObjectNonVersionedBucketAsync()
        {
            try
            {
                var deleteObjectRequest = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };

                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(deleteObjectRequest);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
        }
    }
}
```

Example Suppression d'un objet d'un compartiment activé pour la gestion des versions

L'exemple C# suivant supprime un objet d'un compartiment activé pour la gestion des versions. L'exemple supprime une version de l'objet en spécifiant le nom de la clé d'objet et l'ID de version.

Le code exécute les tâches suivantes :

1. Active la gestion des versions S3 sur un compartiment que vous spécifiez (si la gestion des versions S3 est déjà activée, cette opération est sans effet).
2. Ajoute un exemple d'objet au compartiment. En réponse, Amazon S3 renvoie l'ID de version de l'objet nouvellement ajouté. L'exemple utilise l'ID de version dans la demande de suppression.

3. Supprime l'exemple d'objet en spécifiant le nom de la clé d'objet et l'ID de version.

> **Note**
>
> Vous pouvez également obtenir l'ID de version d'un objet en envoyant une demande `ListVersions`.
>
> ```
> var listResponse = client.ListVersions(new ListVersionsRequest { BucketName
>  = bucketName, Prefix = keyName });
> ```

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class DeleteObjectVersion
    {
        private const string bucketName = "*** versioning-enabled bucket name ***";
        private const string keyName = "*** Object Key Name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateAndDeleteObjectVersionAsync().Wait();
        }

        private static async Task CreateAndDeleteObjectVersionAsync()
        {
            try
```

```
            {
                // Add a sample object.
                string versionID = await PutAnObject(keyName);

                // Delete the object by specifying an object key and a version ID.
                DeleteObjectRequest request = new DeleteObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    VersionId = versionID
                };
                Console.WriteLine("Deleting an object");
                await client.DeleteObjectAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 deleting an object", e.Message);
            }
        }

        static async Task<string> PutAnObject(string objectKey)
        {
            PutObjectRequest request = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = objectKey,
                ContentBody = "This is the content body!"
            };
            PutObjectResponse response = await client.PutObjectAsync(request);
            return response.VersionId;
        }
    }
}
```

PHP

Cet exemple montre comment utiliser les classes de la version 3 de AWS SDK pour PHP pour supprimer un objet d'un bucket non versionné. Pour en savoir plus sur la suppression d'un objet à partir d'un compartiment activé pour la gestion des versions, consultez Utilisation de l'API REST.

Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

L'exemple de PHP suivant supprime un objet à partir d'un compartiment. Comme cet exemple illustre la façon de supprimer des objets des compartiments désactivés pour la gestion des versions, il fournit uniquement le nom du compartiment et la clé d'objet (pas un ID de version) dans la demande de suppression.

```
<?php

require 'vendor/autoload.php';

use Aws\S3\S3Client;
use Aws\S3\Exception\S3Exception;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// 1. Delete the object from the bucket.
try
{
    echo 'Attempting to delete ' . $keyname . '...' . PHP_EOL;

    $result = $s3->deleteObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    if ($result['DeleteMarker'])
    {
        echo $keyname . ' was deleted or does not exist.' . PHP_EOL;
    } else {
        exit('Error: ' . $keyname . ' was not deleted.' . PHP_EOL);
```

```
    }
}
catch (S3Exception $e) {
    exit('Error: ' . $e->getAwsErrorMessage() . PHP_EOL);
}

// 2. Check to see if the object was deleted.
try
{
    echo 'Checking to see if ' . $keyname . ' still exists...' . PHP_EOL;

    $result = $s3->getObject([
        'Bucket' => $bucket,
        'Key'    => $keyname
    ]);

    echo 'Error: ' . $keyname . ' still exists.';
}
catch (S3Exception $e) {
    exit($e->getAwsErrorMessage());
}
```

Javascript

```
import { DeleteObjectCommand } from "@aws-sdk/client-s3";
import { s3Client } from "./libs/s3Client.js" // Helper function that creates Amazon
 S3 service client module.

export const bucketParams = { Bucket: "BUCKET_NAME", Key: "KEY" };

export const run = async () => {
  try {
    const data = await s3Client.send(new DeleteObjectCommand(bucketParams));
    console.log("Success. Object deleted.", data);
    return data; // For unit tests.
  } catch (err) {
    console.log("Error", err);
  }
};
run();
```

Suppression de plusieurs objets

Etant donné que tous les objets dans le compartiment S3 entraînent des coûts de stockage, vous devez supprimer ceux dont vous n'avez plus besoin. Par exemple, si vous collectez des fichiers journaux, vous pouvez les supprimer lorsque vous n'en avez plus besoin. Vous pouvez configurer une règle de cycle de vie pour supprimer automatiquement les objets tels que les fichiers journaux. Pour plus d'informations, consultez the section called "Définition d'une configuration de cycle de vie".

Pour en savoir plus sur les fonctions et la tarification d'Amazon S3, veuillez consulter Tarification Amazon S3.

Vous pouvez utiliser la console Amazon S3 ou l'API REST pour supprimer plusieurs objets simultanément d'un compartiment S3. AWS SDKs

Utilisation de la console S3

Procédez comme suit pour utiliser la console Amazon S3 afin de supprimer plusieurs objets d'un compartiment.

Warning

- La suppression d'un objet spécifié ne peut pas être annulée.
- Cette action supprime tous les objets spécifiés. Lorsque vous supprimez des dossiers, attendez la fin de l'action de suppression pour ajouter de nouveaux objets au dossier. Dans le cas contraire, de nouveaux objets pourraient également être supprimés.
- Lorsque vous supprimez des objets dans un compartiment sans activation de la gestion des versions, y compris des compartiments de répertoire, Amazon S3 supprime définitivement les objets.
- Si vous supprimez des objets d'un compartiment pour lequel la gestion des versions est activée ou suspendue, Amazon S3 crée des marqueurs de suppression. Pour plus d'informations, consultez Utilisation des marqueurs de suppression.

Pour supprimer des objets pour lesquels la gestion des versions est activée ou suspendue

Note

Si la version IDs de l'objet dans un compartiment suspendu aux versions est marquée commeNULL, S3 supprime définitivement les objets car aucune version précédente n'existe.

Toutefois, si un ID de version valide est répertorié pour les objets dans un compartiment pour lequel la gestion des versions est suspendue, S3 crée un marqueur de suppression pour les objets supprimés, tout en conservant les versions précédentes de l'objet.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment dont vous souhaitez supprimer les objets.
4. Sélectionnez les objets, puis choisissez Supprimer.
5. Pour confirmer la suppression de la liste d'objets sous Objets spécifiés dans la zone de texte Supprimer les objets ?, entrez **`delete`**.

Pour supprimer définitivement des versions d'objet spécifiques dans un compartiment pour lequel la gestion des versions est activée

⚠ Warning

Lorsque vous supprimez définitivement des versions d'objets spécifiques dans Amazon S3, cette opération est irréversible.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment dont vous souhaitez supprimer les objets.
4. Sélectionnez les objets que vous voulez supprimer.
5. Choisissez le bouton Afficher les versions.
6. Sélectionnez les versions de l'objet, puis choisissez Supprimer.
7. Pour confirmer la suppression définitive des versions d'objets spécifiques répertoriées sous Objets spécifiés, dans la zone de texte Supprimer les objets ?, entrez Supprimer définitivement. Amazon S3 supprime définitivement ces versions spécifiques de l'objet.

Pour supprimer définitivement les objets d'un compartiment Amazon S3 pour lesquels la gestion des versions n'est pas activée

> **Warning**
>
> Lorsque vous supprimez définitivement un objet dans Amazon S3, cette opération est irréversible. De même, pour tous les compartiments dont la gestion des versions n'est pas activée, y compris les compartiments de répertoire, les suppressions sont permanentes.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment dont vous souhaitez supprimer les objets.
4. Sélectionnez les objets, puis choisissez Supprimer.
5. Pour confirmer la suppression définitive des objets répertoriés sous Objets spécifiés, dans la zone de texte Supprimer des objets ?, entrez Supprimer définitivement.

> **Note**
>
> Si vous rencontrez des problèmes lors de la suppression des objets, consultez Je souhaite supprimer définitivement les objets avec la gestion des versions.

À l'aide du AWS SDKs

Pour des exemples de suppression de plusieurs objets avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Utilisation de l'API REST

Vous pouvez utiliser le AWS SDKs pour supprimer plusieurs objets à l'aide de l'API Multi-Object Delete. Toutefois, si l'application l'exige, vous pouvez envoyer directement des demandes REST.

Pour plus d'informations, consultez Suppression de plusieurs objets dans la Référence d'API Amazon Simple Storage Service.

Organisation, liste et utilisation de vos objets

Dans Amazon S3, vous pouvez utiliser des préfixes pour organiser votre stockage. Un préfixe est un regroupement logique des objets dans un compartiment. La valeur de préfixe est semblable à un nom de répertoire qui vous permet de stocker des données similaires sous le même répertoire d'un compartiment. Lorsque vous chargez des objets par programme, vous pouvez utiliser des préfixes pour organiser vos données.

Dans la console Amazon S3, les préfixes sont appelés dossiers. Vous pouvez afficher tous vos objets et dossiers dans la console S3 en accédant à un compartiment. Vous pouvez également afficher des informations sur chaque objet, y compris les propriétés de l'objet.

Pour en savoir plus sur l'élaboration de liste et l'organisation de vos données dans Amazon S3, consultez les rubriques suivantes.

Rubriques

- Organisation des objets à l'aide de préfixes
- Liste des clés d'objet par programme
- Organisation des objets dans la console Amazon S3 à l'aide de dossiers
- Affichage des propriétés d'un objet dans la console Amazon S3
- Catégorisation de vos objets à l'aide de balises

Organisation des objets à l'aide de préfixes

Vous pouvez utiliser des préfixes pour organiser les données que vous stockez dans des compartiments Amazon S3. Un préfixe est une chaîne de caractères au début du nom de la clé d'objet. Il n'a pas de limite de longueur, mais ne peut pas dépasser la longueur du nom de la clé d'objet (1 024 octets). Vous pouvez voir les préfixes comme un moyen d'organiser vos données de la même manière que les répertoires. Toutefois, les préfixes ne sont pas des répertoires.

La recherche par préfixe limite les résultats aux seules clés qui commencent par le préfixe spécifié. Le délimiteur permet à la liste de regrouper toutes les clés qui partagent un préfixe commun dans une seule liste de résultats récapitulative.

L'objectif des paramètres de préfixe et de délimiteur est de vous aider à organiser et à parcourir hiérarchiquement les clés. Pour ce faire, choisissez tout d'abord un délimiteur pour le compartiment, comme une barre oblique (/), qui n'est présent dans aucun des noms de clés anticipés. Vous pouvez utiliser un autre caractère comme délimiteur. La barre oblique (/) n'est pas unique, mais elle est un délimiteur de préfixe très courant. Ensuite, créez les noms de clés en concaténant tous les niveaux de contenu de la hiérarchie, en séparant chaque niveau avec le délimiteur.

Par exemple, si vous stockez des informations sur des villes, vous devez naturellement les organiser par continent, puis par pays, puis par province ou état. Étant donné que ces noms ne contiennent généralement pas de ponctuation, vous devez utiliser une barre oblique (/) comme délimiteur. Les exemples suivants utilisent une barre oblique (/) comme délimiteur.

- Europe/France/Nouvelle-Aquitaine/Bordeaux
- Nord America/Canada/Quebec/Montreal
- Nord America/USA/Washington/Bellevue
- Nord America/USA/Washington/Seattle

Si vous stockez des données pour chaque ville du monde de cette façon, il apparaît curieux de gérer un espace de noms de clé horizontal. Grâce au `Prefix` et au `Delimiter` avec l'opération de la liste, vous pouvez utiliser la hiérarchie que vous avez créée pour lister les données. Par exemple, pour lister tous les États des États-Unis, configurez `Delimiter='/'` et `Prefix='North America/USA/'`. Pour lister toutes les provinces du Canada pour lesquelles vous avez des données, configurez `Delimiter='/'` et `Prefix='North America/Canada/'`.

Pour plus d'informations sur les délimiteurs, les préfixes et les dossiers imbriqués, consultez Difference between prefixes and nested folders (Différence entre les préfixes et les dossiers imbriqués).

Liste d'objets à l'aide de préfixes et de délimiteurs

Si vous demandez une liste avec un délimiteur, vous pouvez parcourir la hiérarchie sur un seul niveau en passant et en résumant les (éventuels millions de) clés qui se trouvent dans les niveaux suivants. Par exemple, supposons que vous avez un compartiment (*`amzn-s3-demo-bucket`*) avec les clés suivantes :

```
sample.jpg

photos/2006/January/sample.jpg

photos/2006/February/sample2.jpg

photos/2006/February/sample3.jpg

photos/2006/February/sample4.jpg
```

L'exemple de compartiment ne dispose que de l'objet `sample.jpg` à la racine. Pour lister uniquement les objets au niveau racine du compartiment, vous envoyez une demande GET sur le compartiment avec la barre oblique (/) comme délimiteur. En réponse, Simple Storage Service (Amazon S3) renvoie la clé de l'objet `sample.jpg` car elle ne contient pas le délimiteur `/`. Toutes les autres clés contiennent le délimiteur. Simple Storage Service (Amazon S3) regroupe ces clés et renvoie un seul élément `CommonPrefixes` avec la valeur de préfixe `photos/`, qui est une sous-chaîne du début de ces clés jusqu'à la première occurrence du délimiteur spécifié.

Example

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>amzn-s3-demo-bucket</Name>
  <Prefix></Prefix>
  <Marker></Marker>
  <MaxKeys>1000</MaxKeys>
  <Delimiter>/</Delimiter>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>sample.jpg</Key>
    <LastModified>2011-07-24T19:39:30.000Z</LastModified>
    <ETag>&quot;d1a7fb5eab1c16cb4f7cf341cf188c3d&quot;</ETag>
    <Size>6</Size>
    <Owner>
      <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
      <DisplayName>displayname</DisplayName>
    </Owner>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
  <CommonPrefixes>
    <Prefix>photos/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

Pour plus d'informations sur la liste des clés d'objet par programme, consultez Liste des clés d'objet par programme.

Liste des clés d'objet par programme

Dans Amazon S3, les clés peuvent être répertoriées par préfixe. Vous pouvez choisir un préfixe commun pour les noms des clés associées et marquer ces clés avec un caractère spécial délimitant la hiérarchie. Vous pouvez ensuite utiliser l'opération de liste pour sélectionner et parcourir les clés de manière hiérarchique. Cette méthode ressemble au stockage des fichiers dans les répertoires d'un système de fichiers.

Amazon S3 expose une opération de liste qui vous permet d'énumérer les clés contenues dans un compartiment. Les clés sont sélectionnées par compartiment et préfixe. Par exemple, prenez un compartiment appelé « `dictionary` » qui contient une clé pour chaque mot anglais. Vous devez faire un appel pour lister toutes les clés dans le compartiment qui commencent par la lettre « q ». Les résultats de la liste sont toujours renvoyés dans un ordre binaire UTF-8.

Les opérations de la liste SOAP et REST renvoient un document XML qui contient les noms des clés correspondantes et les informations sur l'objet identifié par chaque clé.

> **Note**
>
> Les SOAP APIs pour Amazon S3 ne sont pas disponibles pour les nouveaux clients et approchent de leur fin de vie (EOL) le 31 août 2025. Nous vous recommandons d'utiliser l'API REST ou le AWS SDKs.

Les groupes de clés qui partagent un préfixe se terminant par un délimiteur spécial peuvent être regroupés par ce préfixe commun pour les besoins de la liste. Cela permet aux applications d'organiser et de parcourir hiérarchiquement les clés, comme vous organiseriez des fichiers dans les répertoires d'un système de fichiers.

Par exemple, pour que le compartiment dictionnaire contienne plus que des mots anglais, vous devez former des clés en ajoutant un préfixe à chaque mot avec sa langue et un délimiteur, comme « `French/logical` ». Grâce à cette dénomination et à la fonction de liste hiérarchique, vous pouvez récupérer une liste de mots français. Vous pouvez également parcourir la liste de niveau supérieur des langues disponibles sans avoir à itérer sur toutes les clés d'intervention de manière lexicographique. Pour en savoir plus sur cet aspect de la liste, consultez Organisation des objets à l'aide de préfixes.

API REST

Si l'application l'exige, vous pouvez envoyer les demandes REST directement. Vous pouvez envoyer une demande GET pour renvoyer tout ou partie des objets d'un compartiment. Vous pouvez aussi utiliser des critères de sélection pour renvoyer un sous-ensemble d'objets d'un compartiment. Pour plus d'informations, consultez GET Bucket (List Objects) version 2 dans la Référence d'API Amazon Simple Storage Service.

Efficacité de l'implémentation d'une liste

Les performances de la liste ne sont pas significativement affectées par le nombre total de clés dans votre compartiment. Elles ne sont pas non plus affectées par la présence ou l'absence des arguments `prefix`, `marker`, `maxkeys`, ou `delimiter`.

Itération sur des résultats de plusieurs pages

Etant donné que les compartiments peuvent contenir un nombre presque illimité de clés, les résultats complets d'une requête de liste peuvent être très importants. Pour gérer d'importants ensembles de résultats, l'API Amazon S3 prend en charge la pagination afin de les scinder en plusieurs réponses. Chaque réponse de clés de liste renvoie une page de 1 000 clés maximum avec un indicateur spécifiant si la réponse est tronquée. Vous envoyez une série de demandes de clés de liste jusqu'à ce que vous ayez reçu toutes les clés. AWS Les bibliothèques wrapper du SDK fournissent la même pagination.

Exemples

Lorsque vous répertoriez tous les objets de votre compartiment, notez que vous devez disposer de l'autorisation `s3:ListBucket`.

CLI

list-objects

L'exemple suivant utilise la commande `list-objects` pour afficher le nom de tous les objets du compartiment spécifié :

```
aws s3api list-objects --bucket text-content --query 'Contents[].{Key: Key, Size:
 Size}'
```

L'exemple utilise l'argument `--query` pour filtrer la sortie `list-objects` jusqu'à la valeur de clé et la taille de chaque objet.

Pour en savoir plus sur les objets, consultez Utilisation des objets dans Amazon S3.

- Pour plus de détails sur l'API, reportez-vous ListObjectsà la section Référence des AWS CLI commandes.

ls

L'exemple suivant répertorie tous les objets et préfixes d'un compartiment à l'aide de la commande `ls`.

Pour utiliser cet exemple de commande, remplacez *amzn-s3-demo-bucket* par le nom de votre compartiment.

```
$ aws s3 ls s3://amzn-s3-demo-bucket
```

- Pour plus d'informations sur la commande de haut niveau `ls`, consultez Répertorier les compartiments et les objets dans le Guide de l'utilisateur AWS Command Line Interface .

PowerShell

Outils pour PowerShell V4

Exemple 1 : Cette commande récupère les informations relatives à tous les éléments du compartiment « test-files ».

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

Exemple 2 : Cette commande récupère les informations relatives à l'élément « sample.txt » depuis le compartiment « test-files ».

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```

Exemple 3 : Cette commande récupère les informations relatives à tous les éléments portant le préfixe « sample » à partir du compartiment « test-files ».

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- Pour plus de détails sur l'API, reportez-vous ListObjectsà la section Référence des Outils AWS pour PowerShell applets de commande (V4).

Outils pour PowerShell V5

Exemple 1 : Cette commande récupère les informations relatives à tous les éléments du compartiment « test-files ».

```
Get-S3Object -BucketName amzn-s3-demo-bucket
```

Exemple 2 : Cette commande récupère les informations relatives à l'élément « sample.txt » depuis le compartiment « test-files ».

```
Get-S3Object -BucketName amzn-s3-demo-bucket -Key sample.txt
```

Exemple 3 : Cette commande récupère les informations relatives à tous les éléments portant le préfixe « sample » à partir du compartiment « test-files ».

```
Get-S3Object -BucketName amzn-s3-demo-bucket -KeyPrefix sample
```

- Pour plus de détails sur l'API, reportez-vous ListObjectsà la section Référence des Outils AWS pour PowerShell applets de commande (V5).

Organisation des objets dans la console Amazon S3 à l'aide de dossiers

Dans les compartiments à usage général Amazon S3, les objets sont les principales ressources et les objets sont stockés dans des compartiments. Les compartiments à usage général Amazon S3 ont une structure plate au lieu d'une hiérarchie comme c'est le cas dans un système de fichiers. Toutefois, par souci de simplification organisationnelle, la console Amazon S3 supporte le concept de dossier comme moyen de regrouper des objets. Pour ce faire, la console utilise un préfixe de nom partagé pour les objets groupés. En d'autres termes, les objets de groupe ont des noms qui commencent par une chaîne commune. Cette chaîne commune, ou préfixe partagé, est le nom du dossier. Les noms d'objet sont également appelés noms de clé.

Par exemple, vous pouvez créer un dossier dans un compartiment à usage général de la console nommée `photos` et y stocker un objet nommé`myphoto.jpg`. L'objet est ensuite stocké avec le nom de clé `photos/myphoto.jpg`, dans lequel le préfixe est `photos/`.

Voici deux exemples supplémentaires :

- Si vous avez trois objets dans votre compartiment à usage général (`logs/date1.txt`,`logs/date2.txt`, et`logs/date3.txt`), la console affichera un dossier nommé`logs`. Si vous ouvrez le dossier dans la console, vous voyez les trois objets : `date1.txt`, `date2.txt` et `date3.txt`.
- Si un objet est nommé`photos/2017/example.jpg`, la console affiche un dossier nommé `photos` qui contient le dossier`2017`. Le dossier `2017` contient l'objet`example.jpg`.

Vous pouvez avoir des dossiers dans d'autres dossiers, mais pas de compartiments dans d'autres compartiments. Vous pouvez charger et copier des objets directement dans un dossier. Les dossiers peuvent être créés, supprimés et rendus publics, mais ils ne peuvent pas être renommés. Des objets peuvent être copiés d'un dossier vers un autre.

Important

Lorsque vous créez un dossier dans la console Amazon S3, S3 crée un objet de 0 octet. Cette clé d'objet est définie sur le nom du dossier que vous avez fourni, suivi d'une barre oblique (/). Par exemple, dans la console Amazon S3, si vous créez un dossier nommé `photos` dans votre compartiment, la console Amazon S3 crée un objet de 0 octet avec la clé`photos/`. La console crée cet objet pour prendre en charge les dossiers.
En outre, tout objet préexistant nommé par une barre oblique (/) apparaît sous forme de dossier dans la console Amazon S3. Par exemple, un objet portant le nom de clé `examplekeyname/` apparaît sous forme de dossier dans la console Amazon S3 et non en tant qu'objet. Sinon, il se comporte comme n'importe quel autre objet et peut être visualisé et manipulé via l'API AWS Command Line Interface (AWS CLI) ou REST. AWS SDKs En outre, vous ne pouvez pas télécharger un objet dont le nom de clé est suivi d'une barre oblique (/) à l'aide de la console Amazon S3. Cependant, vous pouvez télécharger des objets nommés par une barre oblique (/) à l'aide de l'API AWS Command Line Interface (AWS CLI) ou REST. AWS SDKs
De plus, la console Amazon S3 n'affiche pas le contenu et les métadonnées des objets de dossier comme elle le fait pour les autres objets. Lorsque vous utilisez la console pour copier un objet nommé avec une barre oblique (/), un nouveau dossier est créé dans l'emplacement de destination, mais les données et métadonnées de l'objet ne sont pas copiées. En outre, une barre oblique (/) dans les noms de clés d'objets peut nécessiter un traitement spécial. Pour de plus amples informations, veuillez consulter Attribution d'un nom aux objets Amazon S3.

Pour créer des dossiers dans des compartiments de répertoires, chargez un dossier. Pour de plus amples informations, veuillez consulter Chargement d'objets dans un compartiment de répertoires.

Rubriques

- Création d'un dossier
- Rendre les dossiers publics
- Calcul de la taille d'un dossier
- Suppression de dossiers

Création d'un dossier

Cette section décrit comment utiliser la console Simple Storage Service (Amazon S3) pour créer un dossier.

> **Important**
>
> Si votre politique de compartiment empêche le chargement d'objets dans ce compartiment sans balises, métadonnées ni bénéficiaires de liste de contrôle d'accès (ACL), vous ne pouvez pas créer de dossier à l'aide de la procédure suivante. Au lieu de cela, chargez un dossier vide et spécifiez les paramètres suivants dans la configuration de chargement.

Pour créer un dossier

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment dans lequel vous souhaitez créer un dossier.
4. Dans l'onglet Objets, choisissez Créer un dossier.
5. Attribuez un nom au dossier (par exemple, **`favorite-pics`**).

> **Note**
>
> Les noms de dossiers sont soumis à certaines limites et directives, et sont considérés comme faisant partie du nom de clé d'objet d'un objet, qui est limité à 1 024 octets. Pour

de plus amples informations, veuillez consulter the section called "Attribution d'un nom aux objets".

6. (Facultatif) Si votre politique de compartiment exige que les objets soient chiffrés avec une clé de chiffrement spécifique, sous Chiffrement côté serveur, vous devez choisir Spécifier une clé de chiffrement et spécifier la même clé de chiffrement lorsque vous créez un dossier. Dans le cas contraire, la création du dossier échouera.
7. Choisissez Créer un dossier.

Rendre les dossiers publics

Nous vous recommandons de bloquer tout l'accès public à vos dossiers et compartiments Amazon S3, à moins que vous ayez besoin spécifiquement d'un dossier ou compartiment public. Lorsque vous rendez public un dossier, quiconque sur Internet peut voir tous les objets qui sont regroupés dans ce dossier.

Dans la console Amazon S3, vous pouvez rendre public un dossier. Vous pouvez également rendre public un dossier en créant une politique de compartiment qui limite l'accès aux données par préfixe. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon S3.

> **Warning**
>
> Une fois que vous avez rendu public un dossier dans la console Amazon S3, vous ne pouvez pas le rendre à nouveau privé. Au lieu de cela, vous devez définir des autorisations sur chaque objet individuel dans le dossier public de sorte que les objets n'aient pas d'accès public. Pour plus d'informations, consultez Configuration ACLs.

Rubriques

- Calcul de la taille d'un dossier
- Suppression de dossiers

Calcul de la taille d'un dossier

Cette section décrit comment utiliser la console Amazon S3 pour calculer la taille d'un dossier.

Pour calculer la taille d'un dossier

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments à usage général, choisissez le nom du compartiment dans lequel votre dossier est stocké.
4. Dans la liste des objets, cochez la case à côté du nom du dossier.
5. Choisissez Actions, puis Calculate total size (Calculer la taille totale).

> **Note**
>
> Lorsque vous quittez la page, les informations du dossier (y compris la taille totale) ne sont plus disponibles. Vous devez recalculer la taille totale si vous souhaitez la voir à nouveau.

> **Important**
>
> Lorsque vous utilisez l'action Calculate total size (Calculer la taille totale) sur des objets ou des dossiers spécifiés dans votre compartiment, Amazon S3 calcule le nombre total d'objets et la taille de stockage totale. Toutefois, les téléchargements partitionnés incomplets ou en cours et les versions précédentes ou anciennes ne sont pas inclus dans le calcul du nombre total d'objets ou de la taille totale. Cette action calcule uniquement le nombre total d'objets et la taille totale pour la version actuelle ou la plus récente de chaque objet stocké dans le compartiment.
>
> Par exemple, si votre compartiment contient deux versions d'un même objet, le calculateur de stockage d'Amazon S3 les compte comme un seul objet. Par conséquent, le nombre total d'objets calculé dans la console Amazon S3 peut différer du nombre d'objets indiqué dans S3 Storage Lens et du nombre indiqué par l' CloudWatch indicateur Amazon,`NumberOfObjects`. De même, la taille de stockage totale peut également différer de la métrique de stockage total indiquée dans S3 Storage Lens et de la `BucketSizeBytes` métrique indiquée dans CloudWatch.

Suppression de dossiers

Cette section explique comment utiliser la console Amazon S3 pour supprimer des dossiers d'un compartiment S3.

Pour plus d'informations sur les fonctionnalités et la tarification d'Amazon S3, consultez Amazon S3.

Pour supprimer des dossiers d'un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments à usage général, choisissez le nom du compartiment dont vous souhaitez supprimer des dossiers.
4. Dans la liste des objets, cochez les cases à côté des dossiers et des objets que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Sur la page Supprimer des objets, vérifiez que les noms des dossiers et des objets que vous avez sélectionnés pour suppression sont répertoriés sous Objets spécifiés.
7. Dans la zone Supprimer les objets, saisissez **`delete`**, et choisissez Supprimer les objets.

> **Warning**
>
> Cette action supprime tous les objets spécifiés. Lorsque vous supprimez des dossiers, attendez la fin de l'action de suppression pour ajouter de nouveaux objets au dossier. Dans le cas contraire, de nouveaux objets pourraient également être supprimés.

Affichage des propriétés d'un objet dans la console Amazon S3

Vous pouvez utiliser la console Amazon S3 pour afficher les propriétés d'un objet, y compris la classe de stockage, les paramètres de chiffrement, les étiquettes et les métadonnées.

Pour afficher les propriétés d'un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant l'objet.
4. Dans la liste Objets, choisissez le nom de l'objet pour lequel vous souhaitez afficher les propriétés.

   La Présentation de l'objet de votre objet s'ouvre. Vous pouvez faire défiler l'écran vers le bas pour afficher les propriétés de l'objet.
5. Sur la page d'aperçu de l'objet, vous pouvez afficher ou configurer les propriétés suivantes pour l'objet.

   > **Note**
   >
   > - Si vous modifiez les propriétés Storage Class (Classe de stockage), Encryption (Chiffrement) et Metadata (Métadonnées), un nouvel objet est créé pour remplacer l'ancien. Si la gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).
   > - Si vous modifiez les propriétés Classe de stockage, Chiffrement ou Métadonnées d'un objet doté de balises définies par l'utilisateur, vous devez disposer de l'autorisation `s3:GetObjectTagging`. Si vous modifiez ces propriétés pour un objet qui ne possède pas de balises définies par l'utilisateur mais dont la taille est supérieure à 16 Mo, vous devez également disposer de l'autorisation `s3:GetObjectTagging`.
   >
   >   Si la politique du compartiment de destination refuse l'action `s3:GetObjectTagging`, ces propriétés de l'objet seront mises à jour, mais les balises définies par l'utilisateur seront supprimées de l'objet et vous recevrez un message d'erreur.

   a. Storage Class (Classe de stockage) – Chaque objet dans Amazon S3 possède une classe de stockage qui lui est associée. La classe de stockage que vous choisissez d'utiliser dépend de la fréquence à laquelle vous accédez à l'objet. La classe de stockage par défaut pour les objets S3 dans des compartiments à usage général est STANDARD. La classe de stockage par défaut pour les objets S3 dans les compartiments de répertoire est S3 Express One Zone. Vous choisissez la classe de stockage à utiliser lors du chargement d'un objet.

Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

Pour modifier la classe de stockage après avoir chargé un objet dans un bucket à usage général, choisissez Classe de stockage. Choisissez la classe de stockage de votre choix, puis cliquez sur Enregistrer.

> **Note**
>
> La classe de stockage des objets dans un compartiment de répertoire ne peut pas être modifiée.

b. Paramètres de chiffrement côté serveur – Vous pouvez utiliser le chiffrement côté serveur pour chiffrer vos objets S3. Pour plus d'informations, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) ou Spécification du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

c. Metadata (Métadonnées) – Chaque objet dans Amazon S3 possède un ensemble de paires nom-valeur qui représente ses métadonnées. Pour en savoir plus sur l'ajout de métadonnées à un objet S3, consultez Modification des métadonnées d'objet dans la console Amazon S3.

d. Balises : vous pouvez classer le stockage en ajoutant des balises à un objet S3 dans un compartiment à usage général. Pour de plus amples informations, veuillez consulter Catégorisation de vos objets à l'aide de balises.

e. Conservation et conservation légales du verrouillage des objets : vous pouvez empêcher la suppression d'un objet d'un bucket à usage général. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

Catégorisation de vos objets à l'aide de balises

Utilisez le balisage des objets pour classer le stockage par catégorie. Chaque balise est une paire clés-valeurs.

Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les chargez ou vous pouvez les ajouter à des objets existants.

- Vous pouvez associer jusqu'à 10 balises à un objet. Les balises associées à un objet doivent avoir des clés de balise uniques.

- Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les balises d'objet Amazon S3 sont représentées en interne en UTF-16. Notez qu'en UTF-16, les caractères occupent une ou deux positions de caractère.
- La clé et les valeurs sont sensibles à la casse.
- Pour plus d'informations sur les restrictions liées aux balises, consultez Restrictions encadrant les balises définies par l'utilisateur dans le Guide de l'utilisateur de Facturation et gestion des coûts AWS . Pour les restrictions de base relatives aux balises, consultez la section Restrictions relatives aux balises dans le guide de EC2 l'utilisateur Amazon.

Exemples

Considérez les exemples de balisage suivants :

Example Informations PHI

Supposons qu'un objet contienne des données relatives aux infos santé protégées (PHI, Protected Health Information). Vous pouvez baliser l'objet à l'aide de la paire clé-valeur suivante.

```
PHI=True
```

ou

```
Classification=PHI
```

Example Fichiers de projet

Supposons que vous stockiez des fichiers de projet dans votre compartiment S3. Vous pouvez baliser ces objets avec une clé nommée `Project` et une valeur, comme illustré ci-après.

```
Project=Blue
```

Example Plusieurs balises

Vous pouvez ajouter plusieurs balises à un objet, comme illustré ci-après.

```
Project=x
Classification=confidential
```

Préfixes de nom de clé et balises

Les préfixes des noms des clés d'objet vous permettent également de classer le stockage. Cependant, le classement basé sur les préfixes est unidimensionnel. Examinez les noms de clés d'objet suivants :

```
photos/photo1.jpg
project/projectx/document.pdf
project/projecty/document2.pdf
```

Ces noms de clés ont les préfixes `photos/`, `project/projectx/` et `project/projecty/`. Ces préfixes permettent un classement par catégorie unidimensionnel. Autrement dit, tout élément sous un préfixe est une catégorie. Par exemple, le préfixe `project/projectx` identifie tous les documents liés au projet x.

Le balisage vous propose maintenant une autre dimension. Si vous souhaitez photo1 dans la catégorie de projet x, vous pouvez baliser l'objet en conséquence.

Autres avantages

Outre la classification des données, le balisage offre d'autres avantages, notamment :

- Les balises d'objets permettent un contrôle d'accès précis des autorisations. Par exemple, vous pouvez accorder à un utilisateur les autorisations de lire uniquement des objets avec des balises spécifiques.
- Les balises d'objets permettent une gestion du cycle de vie des objets précise dans laquelle vous pouvez spécifier un filtre basé sur des balises, en plus du préfixe de nom de clé, dans une règle de cycle de vie.
- Si vous utilisez Analyses Amazon S3, vous pouvez configurer des filtres pour regrouper des objets pour l'analyse par balises d'objets, par préfixe de nom de clé ou à la fois par préfixe et par balises.
- Vous pouvez également personnaliser CloudWatch les statistiques Amazon pour afficher les informations par le biais de filtres de balises spécifiques. Consultez les sections suivantes pour obtenir des détails.

> **Important**
>
> Il est acceptable d'utiliser des balises pour étiqueter des objets contenant des données confidentielles, par exemple, des données d'identification personnelle (PII) ou des

informations santé protégées. Néanmoins, les balises à proprement dit ne doivent pas contenir d'informations confidentielles.

Ajout d'ensembles de balises d'objet à plusieurs objets Amazon S3 avec une seule requête

Pour ajouter des ensembles de balises d'objets à plusieurs objets Amazon S3 avec une seule demande, vous pouvez utiliser la tâche d'opérations par lots S3. Vous fournissez à la fonctionnalité d'opérations par lots S3 une liste d'objets sur lesquels effectuer des opérations. La fonctionnalité des opérations par lot S3 appelle l'opération d'API respective pour effectuer l'opération spécifiée. Une tâche d'opérations par lot peut effectuer l'opération spécifiée sur des milliards d'objets contenant des exaoctets de données.

La fonctionnalité d'opérations par lot S3 suit la progression, envoie des notifications et stocke un rapport de fin détaillé sur toutes les actions, offrant ainsi une expérience sans serveur entièrement gérée et qui peut être vérifiée. Vous pouvez utiliser S3 Batch Operations via la console Amazon S3 ou AWS SDKs l'API REST. AWS CLI Pour de plus amples informations, veuillez consulter the section called "Principes de base des opérations par lot".

Pour en savoir plus sur les balises d'objet, consultez Gestion des balises d'objets.

Opérations API associées au balisage des objets

Amazon S3 prend en charge les opérations API suivantes qui sont spécifiques au balisage des objets :

Opérations d'API sur les objets

- PUT Object Tagging – Remplace les balises sur un objet. Vous spécifiez des balises dans le corps de la demande. Il existe deux scénarios distincts de gestion des balises d'objets à l'aide de cette API.
  - L'objet n'a aucune balise – A l'aide de cette API, vous pouvez ajouter un ensemble de balises à un objet (l'objet n'a pas de balises précédentes).
  - L'objet a un ensemble de balises existantes – Pour modifier l'ensemble de balises existant, vous devez tout d'abord le récupérer, le modifier côté client, puis utiliser cette API pour le remplacer.

    Note

    Si vous envoyez cette demande avec un ensemble de balises vide, Amazon S3 supprime l'ensemble de balises existant de l'objet. Si vous utilisez cette méthode, vous

serez facturé pour une demande de Niveau 1 (PUT). Pour de plus amples informations, veuillez consulter Tarification Amazon S3.
Il est préférable d'utiliser la demande DELETE Object Tagging, car elle produit le même résultat sans entraîner de frais.

- GET Object Tagging – Retourne l'ensemble de balises associé à un objet. Amazon S3 retourne des balises d'objets dans le corps de la réponse.
- DELETE Object Tagging – Supprime l'ensemble de balises associé à un objet.

Autres opérations d'API prenant en charge le balisage

- PUT Object et Initiate Multipart Upload – Vous pouvez spécifier des balises lorsque vous créez des objets. Vous spécifiez les balises à l'aide de l'en-tête de demande `x-amz-tagging`.
- GET Object - Au lieu de retourner l'ensemble de balises, Amazon S3 retourne le nombre de balises d'objets dans l'en-tête `x-amz-tag-count` (uniquement si le demandeur dispose des autorisations de lecture des balises), car la taille de l'en-tête de réponse est limitée à 8 Ko. Si vous souhaitez afficher les balises, vous effectuez une autre demande pour l'opération d'API GET Object Tagging.
- POST Object – Vous pouvez spécifier les balises dans votre demande POST.

  Tant que les balises dans votre demande ne dépassent pas la limite de taille de l'en-tête de demande HTTP de 8 Ko, vous pouvez utiliser l'API `PUT Object` pour créer des objets avec des balises. Si les balises que vous spécifiez dépassent la limite de taille de l'en-tête, vous pouvez utiliser cette méthode POST dans le corps de laquelle vous incluez les balises.

  PUT Object - Copy – Vous pouvez spécifier `x-amz-tagging-directive` dans votre demande pour indiquer à Amazon S3 de copier (comportement par défaut) les balises ou de les remplacer par un nouvel ensemble de balises fourni dans la demande.

Remarques :

- Le balisage d'objet S3 est fortement cohérent. Pour de plus amples informations, veuillez consulter Modèle de cohérence des données Amazon S3.

Configurations supplémentaires

Cette section explique comment le balisage des objets est lié à d'autres configurations.

Balisage des objets et gestion du cycle de vie

Dans la configuration du cycle de vie du compartiment, vous pouvez spécifier un filtre pour sélectionner un sous-ensemble des objets auquel s'applique la règle. Vous pouvez spécifier un filtre basé sur les préfixes des noms de clés, les balises d'objets, ou les deux.

Supposons que vous stockiez des photos (aux formats brut et final) dans votre compartiment Amazon S3. Vous pouvez baliser ces objets comme illustré ci-après.

```
phototype=raw
or
phototype=finished
```

Vous pouvez envisager d'archiver les photos au format brut dans S3 Glacier quelque temps après leur création. Vous pouvez configurer une règle de cycle de vie avec un filtre qui identifie le sous-ensemble des objets avec le préfixe de nom de clé (`photos/`) qui ont une balise spécifique (`phototype=raw`).

Pour de plus amples informations, veuillez consulter Gestion du cycle de vie des objets.

Balisage et réplication d'objets

Si vous avez configuré la réplication sur votre compartiment, Amazon S3 réplique les balises, à condition que vous ayez accordé à Amazon S3 l'autorisation de lire les balises. Pour de plus amples informations, veuillez consulter Présentation de la configuration de la réplication en direct.

Notifications d'événement d'identification d'objet

Vous pouvez configurer une notification d'événement Amazon S3 afin de recevoir une notification lorsqu'une étiquette d'objet est ajoutée ou supprimée d'un objet. Le type d'événement `s3:ObjectTagging:Put` vous avertit lorsqu'une étiquette est PUT sur un objet ou lorsqu'une étiquette existante est mise à jour. Le type d'événement `s3:ObjectTagging:Delete` vous avertit lorsqu'une étiquette est supprimée d'un objet. Pour plus d'informations, consultez Activation des notifications d'événement.

Pour plus d'informations sur le balisage d'objets, consultez les rubriques suivantes :

Rubriques

- Stratégies de balisage et de contrôle d'accès

- Gestion des balises d'objets

Stratégies de balisage et de contrôle d'accès

Vous pouvez également utiliser des stratégies d'autorisations (stratégies de compartiment et stratégies utilisateur) pour gérer les autorisations associées au balisage des objets. Pour les actions des stratégies, consultez les rubriques suivantes :

- Opérations d'objet
- Opérations de compartiment

Les balises d'objets permettent un contrôle d'accès précis pour la gestion des autorisations. Vous pouvez accorder des autorisations conditionnelles basées sur les balises d'objets. Amazon S3 prend en charge les clés de condition suivantes que vous pouvez utiliser pour accorder des autorisations conditionnelles basées sur les balises d'objets.

- `s3:ExistingObjectTag/<tag-key>` – Utilisez cette clé de condition pour vérifier qu'une balise d'objet existante possède la clé de balise et la valeur spécifiques.

  > **Note**
  >
  > Lors de l'octroi des autorisations pour les opérations `PUT Object` et `DELETE Object`, cette clé de condition n'est pas prise en charge. Autrement dit, vous ne pouvez pas créer une stratégie pour accorder ou refuser à un utilisateur les autorisations de supprimer ou de remplacer un objet en fonction de ses balises existantes.

- `s3:RequestObjectTagKeys` – Utilisez cette clé de condition pour limiter les clés de balise que vous voulez autoriser sur les objets. Cela est utile lorsque vous ajoutez des balises à des objets à l'aide PutObjectTagging des PutObject requêtes d'objets and et POST.
- `s3:RequestObjectTag/<tag-key>` – Utilisez cette clé de condition pour limiter les clés de balise et valeurs que vous voulez autoriser sur les objets. Cela est utile lorsque vous ajoutez des balises à des objets à l'aide PutObjectTagging des PutObject requêtes and et POST Bucket.

Pour obtenir la liste complète des clés de condition spécifiques au service Amazon S3, consultez Exemples de politiques de compartiment utilisant des clés de condition. Les stratégies d'autorisations

suivantes illustrent la façon dont le balisage des objets permet une gestion précise des autorisations d'accès.

Example 1 : autoriser un utilisateur à lire uniquement les objets qui ont une valeur de clé et une étiquette spécifiques

La politique d'autorisations suivante limite un utilisateur à la seule lecture des objets qui comportent la clé et la valeur d'étiquette `environment: production`. Cette politique utilise la clé de condition `s3:ExistingObjectTag` pour spécifier la clé et la valeur d'étiquette.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Principal": {
      "AWS": [
        "arn:aws:iam::111122223333:role/JohnDoe"
      ]
    },
    "Effect": "Allow",
    "Action": ["s3:GetObject", "s3:GetObjectVersion"],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
    "Condition": {
      "StringEquals":
        {"s3:ExistingObjectTag/environment": "production"}
    }
  }
  ]
}
```

Example 2 : restreindre les clés d'étiquette d'objet que les utilisateurs peuvent ajouter

La stratégie d'autorisations suivante accorde à un utilisateur les autorisations d'effectuer l'action `s3:PutObjectTagging`, ce qui lui permet d'ajouter des balises à un objet existant. La condition utilise la clé de condition `s3:RequestObjectTagKeys` pour spécifier les clés d'étiquette autorisées, telles que `Owner` ou `CreationDate`. Pour plus d'informations, consultez Création d'une condition avec plusieurs clés ou valeurs dans le Guide de l'utilisateur IAM.

Cette politique garantit que chaque clé d'étiquette spécifiée dans la demande est une clé d'étiquette autorisée. Le qualificateur `ForAnyValue` dans la condition garantit qu'au moins une des clés spécifiées doit être présente dans la demande.

JSON

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
         ]
       },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
            "CreationDate"
          ]
        }
      }
    }
  ]
}
```

Example 3 : exiger une clé et une valeur d'étiquette spécifiques pour permettre aux utilisateurs d'ajouter des étiquettes d'objet

L'exemple de politique suivant accorde à un utilisateur l'autorisation d'exécuter l'action `s3:PutObjectTagging`, qui permet à un utilisateur d'ajouter des étiquettes à un objet existant. La condition exige que l'utilisateur inclue une clé d'étiquette spécifique (telle que *`Project`*) avec la valeur définie sur *`X`*.

JSON

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
         ]
       },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

Gestion des balises d'objets

Cette section explique comment gérer les balises d'objets à l'aide de la console AWS SDKs pour Java et .NET ou de la console Amazon S3.

Le balisage d'objets vous permet de classer le stockage dans des compartiments à usage général. Chaque balise est une paire clé-valeur qui respecte les règles suivantes :

- Vous pouvez associer jusqu'à 10 balises à un objet. Les balises associées à un objet doivent avoir des clés de balise uniques.
- Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les balises d'objet Amazon S3 sont représentées en interne en UTF-16. Notez qu'en UTF-16, les caractères occupent une ou deux positions de caractère.
- La clé et les valeurs sont sensibles à la casse.

Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises. Pour plus d'informations sur les restrictions liées aux balises, consultez Restrictions encadrant les balises définies par l'utilisateur dans le Guide de l'utilisateur AWS Billing and Cost Management .

Utiliser la console S3.

Pour ajouter des balises à un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant l'objet.
4. Cochez la case située à gauche du nom des objets que vous souhaitez modifier.
5. Dans le menu Actions, choisissez Modifier les balises.
6. Vérifiez les objets répertoriés et choisissez Ajouter des balises.
7. Chaque balise d'objet est une paire clé-valeur. Saisissez une Key (Clé) et une Value (Valeur). Choisissez Add Tag (Ajouter une balise) pour ajouter une autre balise.

   Vous pouvez entrer jusqu'à 10 balises pour un objet.
8. Sélectionnez Enregistrer les modifications.

   Amazon S3 ajoute les balises aux objets spécifiés.

Pour plus d'informations, consultez aussi Affichage des propriétés d'un objet dans la console Amazon S3 et Chargement d'objets dans ce guide.

À l'aide du AWS SDKs

Java

L'exemple suivant montre comment utiliser le AWS SDK pour Java pour définir des balises pour un nouvel objet et récupérer ou remplacer des balises pour un objet existant. Pour plus d'informations sur le balisage des objets, consultez Catégorisation de vos objets à l'aide de balises. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
```

```
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.File;
import java.util.ArrayList;
import java.util.List;

public class ManagingObjectTags {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Object key ***";
        String filePath = "*** File path ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Create an object, add two new tags, and upload the object to Amazon
 S3.
            PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
 new File(filePath));
            List<Tag> tags = new ArrayList<Tag>();
            tags.add(new Tag("Tag 1", "This is tag 1"));
            tags.add(new Tag("Tag 2", "This is tag 2"));
            putRequest.setTagging(new ObjectTagging(tags));
            PutObjectResult putResult = s3Client.putObject(putRequest);

            // Retrieve the object's tags.
            GetObjectTaggingRequest getTaggingRequest = new
 GetObjectTaggingRequest(bucketName, keyName);
            GetObjectTaggingResult getTagsResult =
 s3Client.getObjectTagging(getTaggingRequest);

            // Replace the object's tags with two new tags.
            List<Tag> newTags = new ArrayList<Tag>();
            newTags.add(new Tag("Tag 3", "This is tag 3"));
```

```
            newTags.add(new Tag("Tag 4", "This is tag 4"));
            s3Client.setObjectTagging(new SetObjectTaggingRequest(bucketName,
 keyName, new ObjectTagging(newTags)));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

L'exemple suivant montre comment utiliser le AWS SDK pour .NET pour définir les balises d'un nouvel objet et récupérer ou remplacer les balises d'un objet existant. Pour plus d'informations sur le balisage des objets, consultez Catégorisation de vos objets à l'aide de balises.

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    public class ObjectTagsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for the new object ***";
        private const string filePath = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
```

```
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            PutObjectWithTagsTestAsync().Wait();
        }

        static async Task PutObjectWithTagsTestAsync()
        {
            try
            {
                // 1. Put an object with tags.
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    FilePath = filePath,
                    TagSet = new List<Tag>{
                        new Tag { Key = "Keyx1", Value = "Value1"},
                        new Tag { Key = "Keyx2", Value = "Value2" }
                    }
                };

                PutObjectResponse response = await
client.PutObjectAsync(putRequest);
                // 2. Retrieve the object's tags.
                GetObjectTaggingRequest getTagsRequest = new GetObjectTaggingRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };

                GetObjectTaggingResponse objectTags = await
client.GetObjectTaggingAsync(getTagsRequest);
                for (int i = 0; i < objectTags.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
objectTags.Tagging[i].Key, objectTags.Tagging[i].Value);


                // 3. Replace the tagset.

                Tagging newTagSet = new Tagging();
                newTagSet.TagSet = new List<Tag>{
```

```
                    new Tag { Key = "Key3", Value = "Value3"},
                    new Tag { Key = "Key4", Value = "Value4" }
                };


                PutObjectTaggingRequest putObjTagsRequest = new
 PutObjectTaggingRequest()
                {
                    BucketName = bucketName,
                    Key = keyName,
                    Tagging = newTagSet
                };
                PutObjectTaggingResponse response2 = await
 client.PutObjectTaggingAsync(putObjTagsRequest);

                // 4. Retrieve the object's tags.
                GetObjectTaggingRequest getTagsRequest2 = new
 GetObjectTaggingRequest();
                getTagsRequest2.BucketName = bucketName;
                getTagsRequest2.Key = keyName;
                GetObjectTaggingResponse objectTags2 = await
 client.GetObjectTaggingAsync(getTagsRequest2);
                for (int i = 0; i < objectTags2.Tagging.Count; i++)
                    Console.WriteLine("Key: {0}, Value: {1}",
 objectTags2.Tagging[i].Key, objectTags2.Tagging[i].Value);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine(
                        "Error encountered ***. Message:'{0}' when writing an
 object"
                        , e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine(
                    "Encountered an error. Message:'{0}' when writing an object"
                    , e.Message);
            }
        }
    }
}
```

Téléchargez et chargez des objets avec une signature préalable URLs

Vous pouvez utiliser Presigned URLs pour accorder un accès limité dans le temps aux objets dans Amazon S3 sans mettre à jour votre politique de compartiment. Une URL présignée peut être saisie dans un navigateur ou utilisée par un programme pour charger un objet. Les informations d'identification utilisées par l'URL présignée sont celles de l' AWS utilisateur qui a généré l'URL.

Vous pouvez également utiliser Presigned URLs pour autoriser quelqu'un à télécharger un objet spécifique dans votre compartiment Amazon S3. Cela permet un téléchargement sans qu'une autre partie ne doive disposer d'informations d'identification ou d'autorisations de AWS sécurité. Si un objet avec la même clé que celle spécifiée dans l'URL présignée existe déjà dans le compartiment, Amazon S3 remplace l'objet existant par l'objet chargé.

Vous pouvez utiliser l'URL présignée plusieurs fois, jusqu'à la date et l'heure d'expiration.

Lorsque vous créez une URL présignée, vous devez fournir vos informations d'identification de sécurité, puis spécifier les éléments suivants :

- Un compartiment Amazon S3
- Une clé d'objet (si le téléchargement de cet objet se fait dans votre compartiment Amazon S3, s'il s'agit du nom du fichier à charger)
- Une méthode HTTP (`GET`pour télécharger des objets, `PUT` pour télécharger, `HEAD` pour lire les métadonnées des objets, etc.)
- Un intervalle de temps d'expiration

Actuellement, Amazon S3 presigned URLs ne prend pas en charge l'utilisation des algorithmes de somme de contrôle d'intégrité des données suivants (CRC32,, CRC32CSHA-1,SHA-256) lorsque vous chargez des objets. Pour vérifier l'intégrité de votre objet après son chargement, vous pouvez fournir un récapitulatif MD5 de l'objet lorsque vous le chargez avec une URL présignée. Pour en savoir plus sur l'intégrité des objets, consultez Vérification de l'intégrité des objets dans Amazon S3.

Rubriques

- Utilisateurs habilités à créer une URL présignée
- Date d'expiration du présigné URLs
- Limitation des capacités des URL présignées

- Partage d'objets avec présigné URLs
- Téléchargement d'objets présignés URLs

Utilisateurs habilités à créer une URL présignée

Toute personne qui possède des autorisations de sécurité valides peut créer une URL présignée. Mais pour que l'utilisateur puisse accéder correctement à un objet, l'URL présignée doit être créée par une personne qui possède l'autorisation d'effectuer l'opération sur laquelle l'URL présignée est basée.

Les informations d'identification que vous pouvez utiliser pour créer une URL présignée sont les suivantes :

- Profil d'instance IAM : valide pendant 6 heures.
- AWS Security Token Service : valide jusqu'à un maximum de 36 heures en cas de signature avec des informations d'identification de sécurité à long terme ou pendant la durée de validité des informations d'identification temporaires, selon l'élément qui se termine en premier.
- Utilisateur IAM — Valable jusqu'à 7 jours lorsque vous utilisez AWS Signature version 4.

  Afin de créer une URL présignée valide pendant 7 jours maximum, commencez par déléguer des informations d'identification d'utilisateur IAM (clé d'accès et clé secrète) à la méthode que vous utilisez pour créer l'URL présignée.

> **Note**
>
> Si vous avez créé une URL présignée à l'aide d'informations d'identification temporaires, l'URL expire quand les informations d'identification expirent. En général, une URL présignée expire lorsque les informations d'identification que vous avez utilisées pour la créer sont révoquées, supprimées ou désactivées. Cela est vrai même si l'URL a été créée avec une date d'expiration ultérieure. Pour connaître la durée de vie des informations d'identification de sécurité temporaires, consultez la section Comparaison des opérations AWS STS d'API dans le guide de l'utilisateur IAM.

Date d'expiration du présigné URLs

Une URL présignée reste valide pendant la période spécifiée lors de sa génération. Si vous créez une URL présignée à l'aide de la console Amazon S3, le délai d'expiration peut être défini entre 1 minute et 12 heures. Si vous utilisez le AWS CLI ou AWS SDKs, le délai d'expiration peut être fixé à 7 jours.

Si vous avez créé une URL présignée à l'aide d'un jeton temporaire, cette URL expirera quand le jeton expirera. En général, une URL présignée expire lorsque les informations d'identification que vous avez utilisées pour la créer sont révoquées, supprimées ou désactivées. Cela est vrai même si l'URL a été créée avec une date d'expiration ultérieure. Pour plus d'informations sur la manière dont les informations d'identification que vous utilisez affectent le délai d'expiration, consultez Utilisateurs habilités à créer une URL présignée.

Amazon S3 vérifie la date et l'heure d'expiration d'une URL signée au moment de la requête HTTP. Par exemple, si un client commence à télécharger un fichier volumineux immédiatement avant la date d'expiration, le téléchargement continue même si la date d'expiration intervient pendant le téléchargement. Cependant, si la connexion est perdue et que le client essaie de redémarrer le téléchargement une fois la date d'expiration passée, le téléchargement échoue.

Limitation des capacités des URL présignées

Les capacités d'une URL présignée sont limitées par les autorisations de l'utilisateur qui l'a créée. Essentiellement, les jetons présignés URLs sont des jetons porteurs qui donnent accès à ceux qui les possèdent. À ce titre, nous vous recommandons de les protéger de manière appropriée. Voici quelques méthodes que vous pouvez utiliser pour restreindre l'utilisation de votre présigné URLs.

AWS Version 4 de la signature (SigV4)

Pour imposer un comportement spécifique lorsque les requêtes d'URL présignées sont authentifiées à l'aide d' AWS Signature Version 4 (SigV4), vous pouvez utiliser les clés de condition dans les stratégies de compartiment et les stratégies de point d'accès. Par exemple, la politique de compartiment suivante utilise la condition `s3:signatureAge` pour refuser toute demande d'URL présignée Amazon S3 sur les objets du compartiment *`amzn-s3-demo-bucket`* si la signature date de plus de 10 minutes. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Deny a presigned URL request if the signature is more than 10
 min old",
            "Effect": "Deny",
            "Principal": {
                "AWS": "*"
            },
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "NumericGreaterThan": {
                    "s3:signatureAge": "600000"
                }
            }
        }
    ]
}
```

Pour plus d'informations sur les clés de politique relatives à AWS la version 4 de Signature, consultez AWS la section Authentification de signature version 4 dans le manuel Amazon Simple Storage Service API Reference.

Restriction de chemin réseau

Si vous souhaitez restreindre l'utilisation des accès présignés URLs et de tous les accès Amazon S3 à des chemins réseau particuliers, vous pouvez écrire des politiques AWS Identity and Access Management (IAM). Vous pouvez définir ces politiques sur le principal IAM qui effectue l'appel, le compartiment Simple Storage Service (Amazon S3) ou les deux.

Une restriction de chemin réseau sur le principal IAM exige que l'utilisateur de ces informations d'identification effectue des requêtes à partir du réseau spécifié. Une restriction sur le compartiment ou le point d'accès nécessite que toutes les requêtes adressées à cette ressource proviennent du réseau spécifié. Ces restrictions s'appliquent également hors du scénario des URL présignées.

La clé de condition globale IAM que vous utilisez dépend du type de point de terminaison. Si vous utilisez le point de terminaison public pour Amazon S3, utilisez `aws:SourceIp`. Si vous utilisez un point de terminaison de cloud privé virtuel (VPC) pour Amazon S3, utilisez `aws:SourceVpc` ou `aws:SourceVpce`.

La déclaration de politique IAM suivante exige que le principal AWS n'accède qu'à partir de la plage réseau spécifiée. Avec cette déclaration de stratégie, tous les accès doivent provenir de cette plage. Cela inclut lorsqu'une personne utilise une URL présignée pour Amazon S3. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
{
    "Sid": "NetworkRestrictionForIAMPrincipal",
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
        "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
        "BoolIfExists": {"aws:ViaAWSService": "false"}
    }
}
```

Partage d'objets avec présigné URLs

Par défaut, tous les objets Amazon S3 sont privés, seul le propriétaire de l'objet a l'autorisation d'y accéder. Toutefois, le propriétaire de l'objet peut partager des objets avec d'autres personnes en créant une URL présignée. Une URL présignée utilise des informations d'identification de sécurité pour accorder une autorisation limitée dans le temps pour télécharger des objets. L'URL peut être saisie dans un navigateur ou utilisée par un programme pour télécharger l'objet. Les informations d'identification utilisées par l'URL présignée sont celles de l' AWS utilisateur qui a généré l'URL.

Pour des informations générales sur le présigné URLs, consultezTéléchargez et chargez des objets avec une signature préalable URLs.

Vous pouvez créer une URL présignée pour partager un objet sans écrire de code en utilisant la console Amazon S3, AWS Explorer pour Visual Studio (Windows) ou AWS Toolkit for Visual Studio Code. Vous pouvez également générer une URL présignée par programmation en utilisant le AWS Command Line Interface (AWS CLI) ou le. AWS SDKs

Utilisation de la console S3

Vous pouvez utiliser la console Amazon S3 afin de générer une URL présignée pour partager un objet en suivant ces étapes. Dans la console, le délai d'expiration maximal d'une URL présignée est de 12 heures à compter de la création.

Pour générer une URL présignée à l'aide de la console Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments à usage général, choisissez le nom du compartiment à usage général qui contient l'objet pour lequel vous souhaitez obtenir une URL présignée.
4. Dans la liste Objects (Objets), sélectionnez l'objet pour lequel vous souhaitez créer une URL présignée.
5. Dans le menu Actions d'objet, choisissez Partager avec une URL présignée.
6. Spécifiez la durée de validité souhaitée pour l'URL présignée.
7. Choisissez Create presigned URL (Créer une URL présignée).
8. Lorsqu'une confirmation apparaît, l'URL est automatiquement copiée dans votre presse-papier. Un bouton s'affiche pour copier l'URL présignée, si vous devez la copier à nouveau.

À l'aide du AWS CLI

L'exemple de AWS CLI commande suivant génère une URL présignée pour partager un objet depuis un compartiment Amazon S3. Lorsque vous utilisez le AWS CLI, le délai d'expiration maximal d'une URL présignée est de 7 jours à compter de sa création. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800
```

> **Note**
>
> Pour tous Régions AWS ceux lancés après le 20 mars 2019, vous devez spécifier le `endpoint-url` et `Région AWS` avec la demande. Pour voir la liste complète des régions

et points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Référence générale AWS .

```
aws s3 presign s3://amzn-s3-demo-bucket/mydoc.txt --expires-in 604800 --region af-south-1 --endpoint-url https://s3.af-south-1.amazonaws.com
```

Pour plus d'informations, consultez presign dans la Référence des commandes de l'AWS CLI .

À l'aide du AWS SDKs

Vous pouvez générer une URL présignée par programmation à l'aide du. AWS SDKs

Python

Le script Python ci-dessous génère une URL GET présignée pour partager un objet.

1. Copiez le contenu du script et enregistrez-le sous forme de fichier « *get-only-url.py* ». Pour utiliser les exemples suivants, remplacez le *user input placeholders* par vos propres informations (telles que le nom de votre fichier).

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
```

```
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
 '{client_method}'.")
        raise
    return url

def main():
    parser = argparse.ArgumentParser()
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    args = parser.parse_args()

    # By default, this will use credentials from ~/.aws/credentials
    s3_client = boto3.client("s3")

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "get_object",
        {"Bucket": args.bucket, "Key": args.key},
        1000
    )
    print(f"Generated GET presigned URL: {url}")

if __name__ == "__main__":
    main()
```

2. Pour générer une URL GET présignée pour partager un fichier, exécutez le script suivant avec le nom de votre compartiment et le chemin d'objet souhaité.

   La commande suivante utilise des exemples de valeurs. Remplacez *user input placeholders* par vos propres informations.

   ```
   python get-only-url.py amzn-s3-demo-bucket <object-path>
   ```

   Le script affichera une URL GET présignée :

   ```
   Generated GET presigned URL: https://amzn-s3-demo-
   bucket.s3.amazonaws.com/object.txt?AWS
   ```

```
 AccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa
%2ByT372YEAiv4%3D&Expires=1741978496
```

3. Vous pouvez télécharger le fichier en utilisant l'URL présignée générée avec curl :

```
curl -X GET "generated-presigned-url" -o "path/to/save/file"
```

Pour d'autres exemples d'utilisation du AWS SDKs pour générer une URL présignée pour partager un objet, consultez Créer une URL présignée pour Amazon S3 à l'aide d'un AWS SDK.

> **Note**
>
> Pour tous Régions AWS ceux lancés après le 20 mars 2019, vous devez spécifier le `endpoint-url` et `Région AWS` avec la demande. Pour voir la liste complète des régions et points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Référence générale AWS .

> **Note**
>
> Lorsque vous utilisez le AWS SDKs, l'attribut Tagging doit être un en-tête et non un paramètre de requête. Tous les autres attributs peuvent être transmis en tant que paramètre pour l'URL présignée.

À l'aide du AWS Toolkit for Visual Studio (Windows)

> **Note**
>
> À l'heure actuelle, Visual Studio pour Mac AWS Toolkit for Visual Studio n'est pas compatible.

1. Installez le AWS Toolkit for Visual Studio en suivant les instructions ci-dessous, Installation et configuration du Toolkit for Visual Studio dans le guide de AWS Toolkit for Visual Studio l'utilisateur.
2. Connectez-vous à AWS en suivant les étapes ci-dessous, section Connexion à AWS dans le guide de AWS Toolkit for Visual Studio l'utilisateur.

3. Dans le volet latéral gauche intitulé Explorateur AWS , double-cliquez sur le compartiment contenant votre objet.
4. Cliquez avec le bouton droit sur l'objet pour lequel vous souhaitez générer une URL présignée, puis sélectionnez Créer une URL présignée.
5. Dans la fenêtre contextuelle, définissez la date et l'heure d'expiration de votre URL présignée.
6. La clé d'objet devrait être préremplie en fonction de l'objet que vous avez sélectionné.
7. Choisissez GET pour spécifier que cette URL présignée est utilisée pour télécharger un objet.
8. Cliquez sur le bouton Générer.
9. Pour copier l'URL dans le presse-papiers, choisissez Copier.
10. Pour utiliser l'URL présignée générée, collez l'URL dans n'importe quel navigateur.

En utilisant AWS Toolkit for Visual Studio Code

Si vous utilisez Visual Studio Code, vous pouvez générer une URL pré-signée pour partager un objet sans écrire de code grâce à AWS Toolkit for Visual Studio Code. Pour des informations générales, consultez AWS Toolkit for Visual Studio Code dans le Guide de l'utilisateur AWS Toolkit for Visual Studio Code .

Pour obtenir des instructions sur l'installation du AWS Toolkit for Visual Studio Code, reportez-vous à la section Installation du AWS Toolkit for Visual Studio Code dans le guide de AWS Toolkit for Visual Studio Code l'utilisateur.

1. Connectez-vous à AWS en suivant les étapes ci-dessous, section Connexion à AWS Toolkit for Visual Studio Code dans le guide de AWS Toolkit for Visual Studio Code l'utilisateur.
2. Sélectionnez le AWS logo sur le panneau de gauche dans Visual Studio Code.
3. Sous EXPLORER, sélectionnez S3.
4. Choisissez un compartiment et un fichier, puis ouvrez le menu contextuel (clic droit).
5. Choisissez Générer une URL présignée, puis définissez le délai d'expiration (en minutes).
6. Appuyez sur Entrée et l'URL présignée est copiée dans votre presse-papiers.

Téléchargement d'objets présignés URLs

Vous pouvez utiliser Presigned URLs pour autoriser quelqu'un à charger un objet dans votre compartiment Amazon S3. L'utilisation d'une URL présignée permettra un téléchargement sans

qu'une autre partie n'ait besoin d'informations d'identification ou d'autorisations AWS de sécurité. Une URL présignée est limitée par les autorisations de l'utilisateur qui l'a créée. Cela signifie que si vous recevez une URL présignée pour charger un objet, vous pouvez le charger uniquement si le créateur de l'URL dispose des autorisations nécessaires pour charger cet objet.

Lorsqu'une personne utilise l'URL pour charger un objet, Amazon S3 crée l'objet dans le compartiment spécifié. Si un objet avec la même clé que celle spécifiée dans l'URL présignée existe déjà dans le compartiment, Simple Storage Service (Amazon S3) remplace l'objet existant par l'objet chargé. Après le chargement, le propriétaire du compartiment devient propriétaire de l'objet.

Pour des informations générales sur le présigné URLs, consultezTéléchargez et chargez des objets avec une signature préalable URLs.

Vous pouvez créer une URL présignée pour le chargement d'un objet sans écrire de code grâce à AWS Explorer for Visual Studio. Vous pouvez également générer une URL présignée par programmation à l'aide du. AWS SDKs

> **Note**
>
> À l'heure actuelle, Visual Studio pour Mac AWS Toolkit for Visual Studio n'est pas compatible.

À l'aide du AWS Toolkit for Visual Studio (Windows)

1. Installez le AWS Toolkit for Visual Studio en suivant les instructions ci-dessous, Installation et configuration du Toolkit for Visual Studio dans le guide de AWS Toolkit for Visual Studio l'utilisateur.
2. Connectez-vous à AWS en suivant les étapes ci-dessous, section Connexion à AWS dans le guide de AWS Toolkit for Visual Studio l'utilisateur.
3. Dans le volet de gauche intitulé Explorateur AWS , cliquez avec le bouton droit sur le compartiment dans lequel vous souhaitez charger un objet.
4. Choisissez Créer une URL présignée.
5. Dans la fenêtre contextuelle, définissez la date et l'heure d'expiration de votre URL présignée.
6. Pour Clé d'objet, définissez le nom du fichier à charger. Le fichier que vous chargez doit correspondre exactement à ce nom. Si un objet avec la même clé que celle spécifiée dans l'URL présignée existe déjà dans le compartiment, Amazon S3 remplace l'objet existant par l'objet chargé.
7. Choisissez PUT pour spécifier que cette URL présignée est utilisée pour charger un objet.

8. Cliquez sur le bouton Générer.
9. Pour copier l'URL dans le presse-papiers, choisissez Copier.
10. Pour utiliser cette URL, vous pouvez envoyer une demande PUT avec la commande `curl`. Incluez le chemin complet de votre fichier et l'URL présignée elle-même.

```
curl -X PUT -T "/path/to/file" "presigned URL"
```

Utilisation du AWS SDKs pour générer une URL **PUT** présignée pour le téléchargement d'un fichier

Vous pouvez générer une URL présignée qui peut exécuter une action S3 pendant une durée limitée.

> **Note**
>
> Si vous utilisez la AWS CLI ou AWS SDKs, le délai d'expiration du présigné URLs peut être fixé à 7 jours. Pour plus d'informations, consultez la section Délai d'expiration des documents présignés URLs.

Python

Le script Python suivant génère une URL PUT présignée pour le téléchargement d'un objet dans un compartiment S3 à usage général.

1. Copiez le contenu du script et enregistrez-le sous forme de fichier « *put-only-url.py* ». Pour utiliser les exemples suivants, remplacez le *user input placeholders* par vos propres informations (telles que le nom de votre fichier).

```
import argparse
import boto3
from botocore.exceptions import ClientError

def generate_presigned_url(s3_client, client_method, method_parameters,
 expires_in):
    """
    Generate a presigned Amazon S3 URL that can be used to perform an action.

    :param s3_client: A Boto3 Amazon S3 client.
    :param client_method: The name of the client method that the URL performs.
    :param method_parameters: The parameters of the specified client method.
```

```
    :param expires_in: The number of seconds the presigned URL is valid for.
    :return: The presigned URL.
    """
    try:
        url = s3_client.generate_presigned_url(
            ClientMethod=client_method,
            Params=method_parameters,
            ExpiresIn=expires_in
        )
    except ClientError:
        print(f"Couldn't get a presigned URL for client method
 '{client_method}'.")
        raise
    return url

def main():
    parser = argparse.ArgumentParser()
    parser.add_argument("bucket", help="The name of the bucket.")
    parser.add_argument(
        "key", help="The key (path and filename) in the S3 bucket.",
    )
    args = parser.parse_args()

    # By default, this will use credentials from ~/.aws/credentials
    s3_client = boto3.client("s3")

    # The presigned URL is specified to expire in 1000 seconds
    url = generate_presigned_url(
        s3_client,
        "put_object",
        {"Bucket": args.bucket, "Key": args.key},
        1000
    )
    print(f"Generated PUT presigned URL: {url}")

if __name__ == "__main__":
    main()
```

2. Pour générer une URL PUT présignée pour le téléchargement d'un fichier, exécutez le script suivant avec le nom de votre compartiment et le chemin d'objet souhaité.

   La commande suivante utilise des exemples de valeurs. Remplacez *`user input placeholders`* par vos propres informations.

```
python put-only-url.py amzn-s3-demo-bucket <object-path>
```

Le script affichera une URL PUT présignée :

```
Generated PUT presigned URL: https://amzn-s3-demo-
bucket.s3.amazonaws.com/object.txt?AWS
 AccessKeyId=AKIAIOSFODNN7EXAMPLE&Signature=vjbyNxybdZaMmLa
%2ByT372YEAiv4%3D&Expires=1741978496
```

3. Vous pouvez maintenant télécharger le fichier en utilisant l'URL présignée générée avec curl :

```
curl -X PUT -T "path/to/your/local/file" "generated-presigned-url"
```

Pour d'autres exemples d'utilisation du AWS SDKs pour générer une URL présignée pour le téléchargement d'un objet, consultez Créer une URL présignée pour Amazon S3 à l'aide d'un SDK. AWS

Transformation d'objets avec S3 Object Lambda

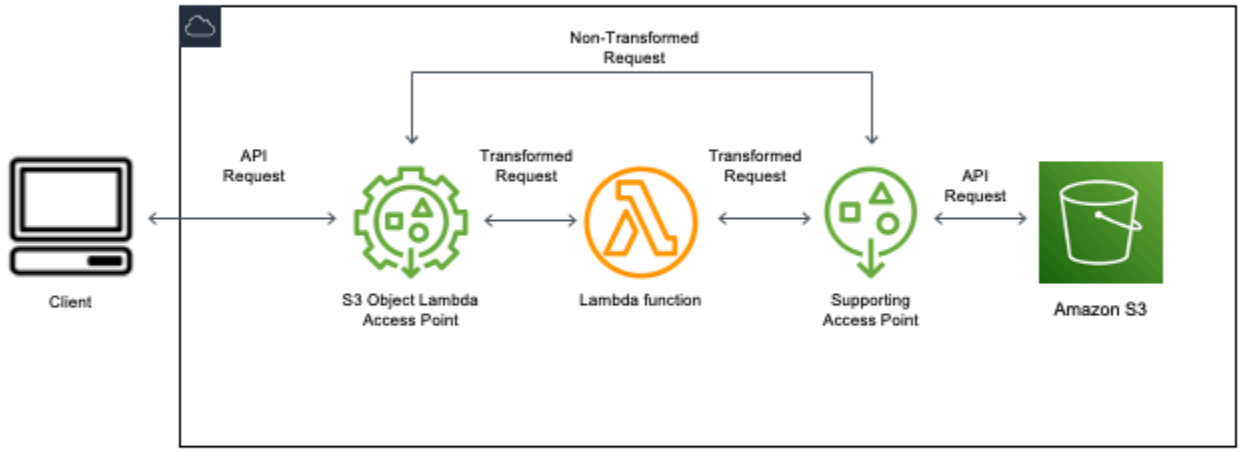
Amazon S3 Object Lambda vous donne la possibilité d'ajouter votre propre code aux requêtes Amazon S3 `GET`, `LIST` et `HEAD` afin de modifier et de traiter les données lorsqu'elles sont renvoyées vers une application. Vous pouvez utiliser du code personnalisé pour modifier les données renvoyées par les demandes S3 `GET` afin de filtrer les lignes, de redimensionner les images et les filigranes de manière dynamique, de supprimer des données confidentielles et plus encore. Vous pouvez également utiliser S3 Object Lambda pour modifier la sortie des requêtes S3 `LIST` afin de créer une vue personnalisée de tous les objets d'un compartiment et des requêtes S3 `HEAD` pour modifier les métadonnées des objets, telles que le nom et la taille des objets. Vous pouvez utiliser S3 Object Lambda comme origine pour votre CloudFront distribution Amazon afin de personnaliser les données pour les utilisateurs finaux, par exemple en redimensionnant automatiquement les images, en transcodant d'anciens formats (comme de JPEG en WebP) ou en supprimant des métadonnées. Pour plus d'informations, consultez le billet de AWS blog Use Amazon S3 Object Lambda with Amazon. CloudFront Alimenté par les fonctions AWS Lambda, votre code s'exécute sur une infrastructure entièrement gérée par. AWS S3 Object Lambda réduit le besoin de créer et de stocker des copies dérivées de vos données ou d'exécuter des proxys, tout cela sans avoir à modifier vos applications.

Fonctionnement de S3 Object Lambda

S3 Object Lambda utilise des AWS Lambda fonctions pour traiter automatiquement la sortie des requêtes S3 ou `HEAD` des `GET` requêtes `LIST` standard. AWS Lambda est un service de calcul sans serveur qui exécute du code défini par le client sans nécessiter la gestion des ressources informatiques sous-jacentes. Vous pouvez créer et exécuter vos propres fonctions Lambda personnalisées afin d'ajuster la transformation des données à vos cas d'utilisation spécifiques.

Après avoir configuré une fonction Lambda, vous l'attachez à un point de terminaison de service S3 Object Lambda (connu sous le nom de point d'accès Object Lambda). Le point d'accès Object Lambda utilise un point d'accès S3 standard, connu sous le nom de point d'accès auxiliaire, pour accéder aux données.

Lorsque vous envoyez une demande à votre point d'accès Object Lambda, Amazon S3 appelle automatiquement votre fonction Lambda. Toutes les données récupérées à l'aide d'une demande S3 `GET`, `LIST` ou `HEAD` via le point de terminaison Object Lambda renvoient un résultat transformé à l'application. Toutes les autres demandes sont traitées comme d'habitude, comme illustré dans le diagramme suivant.



Les rubriques de cette section décrivent comment utiliser S3 Object Lambda.

Rubriques

- Création de points d'accès Object Lambda
- Utilisation des points d'accès Amazon S3 Object Lambda
- Considérations sur la sécurité pour les points d'accès S3 Object Lambda
- Écriture de fonctions Lambda pour les points d'accès S3 Object Lambda
- Utilisation de AWS fonctions Lambda intégrées
- Bonnes pratiques et directives pour S3 Object Lambda
- Didacticiels S3 Object Lambda
- Débogage et résolution des problèmes de S3 Object Lambda

Création de points d'accès Object Lambda

Un point d'accès Object Lambda est associé à un seul point d'accès standard, que vous spécifiez lors de la création. Pour créer un point d'accès Object Lambda, vous avez besoin des ressources suivantes :

- Un point d'accès S3 standard. Lorsque vous travaillez avec des points d'accès Object Lambda, ce point d'accès standard est appelé point d'accès auxiliaire et est attaché à un compartiment S3 ou à un volume Amazon FSx pour OpenZFS. Pour obtenir des informations sur la création de points d'accès standard, consultez the section called "Création d'un point d'accès".
- Une AWS Lambda fonction. Vous pouvez créer votre propre fonction Lambda ou utiliser une fonction prédéfinie. Pour plus d'informations sur la création de fonctions Lambda, consultez the section called "Écriture de fonctions Lambda". Pour plus d'informations sur les fonctions prédéfinies, consultez Utilisation de AWS fonctions Lambda intégrées.
- (Facultatif) Une politique AWS Identity and Access Management (IAM). Les points d'accès Amazon S3 prennent en charge les politiques de ressources IAM que vous pouvez utiliser pour contrôler l'utilisation des points d'accès par ressource, utilisateur ou autres conditions. Pour plus d'informations sur la création de telles politiques, consultez the section called "Configuration des stratégies IAM".

Les sections suivantes décrivent comment créer un point d'accès Object Lambda en utilisant :

- Le AWS Management Console
- Le AWS Command Line Interface (AWS CLI)

- Un AWS CloudFormation modèle
- Le AWS Cloud Development Kit (AWS CDK)

Pour obtenir des informations sur la création d'un point d'accès Object Lambda à l'aide de l'API REST, consultez `CreateAccessPointForObjectLambda` dans la Référence d'API Amazon Simple Storage Service.

Créer un point d'accès Object Lambda

Utilisez l'une des procédures suivantes pour créer votre point d'accès Object Lambda.

Utilisation de la console S3

Pour créer un point d'accès Object Lambda à l'aide de la console

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région à laquelle vous souhaitez passer.
3. Dans le volet de navigation de gauche, choisissez Points d'accès Object Lambda.
4. Dans la page Points d'accès Object Lambda, choisissez Créer un point d'accès Object Lambda.
5. Pour Object Lambda Access Point name (Nom du point d'accès Object Lambda), saisissez le nom que vous souhaitez utiliser pour le point d'accès.

   Comme pour les points d'accès standard, des règles s'appliquent à l'attribution de noms pour des points d'accès Object Lambda. Pour plus d'informations, consultez Règles de dénomination pour les points d'accès.
6. Pour Supporting Access Point (Point d'accès de prise en charge), saisissez le point d'accès standard à utiliser ou accédez-y. Le point d'accès doit se trouver dans le même Région AWS emplacement que les objets que vous souhaitez transformer. Pour obtenir des informations sur la création de points d'accès standard, consultez the section called "Création d'un point d'accès".
7. Sous Configuration de transformation, vous pouvez ajouter une fonction qui transforme vos données pour votre point d'accès Object Lambda. Effectuez l'une des actions suivantes :

   - Si vous avez déjà une AWS Lambda fonction dans votre compte, vous pouvez la sélectionner sous Invoke Lambda function. Vous pouvez saisir ici l'Amazon Resource Name (ARN) d'une

fonction Lambda dans votre Compte AWS ou choisir une fonction Lambda dans le menu déroulant.

- Si vous souhaitez utiliser une fonction AWS intégrée, choisissez le nom de la fonction sous fonction AWS construite et sélectionnez Créer une fonction Lambda. Cela vous mènera à la console Lambda où vous pourrez déployer une fonction intégrée dans votre. Compte AWS Pour plus d'informations sur les fonctions définies, consultez Utilisation de AWS fonctions Lambda intégrées.

Sous S3 APIs, choisissez une ou plusieurs opérations d'API à appeler. Pour chaque API sélectionnée, vous devez spécifier une fonction Lambda à invoquer.

8. (Facultatif) Sous Payload (Charge utile), ajoutez le texte JSON à fournir en entrée à la fonction Lambda. Vous pouvez configurer des charges utiles avec différents paramètres pour différents points d'accès Object Lambda qui invoquent la même fonction Lambda, augmentant ainsi la flexibilité de votre fonction Lambda.

   > **Important**
   >
   > Lorsque vous utilisez des points d'accès Object Lambda, vérifiez que la charge utile ne contient pas d'informations confidentielles.

9. (Facultatif) Pour Range and part number (Plage et numéro de partie), vous devez activer cette option pour traiter les requêtes `GET` et `HEAD` avec des en-têtes de plage et de numéro de partie. L'activation de cette option confirme que votre fonction Lambda est capable de reconnaître et de traiter ces demandes. Pour plus d'informations sur les en-têtes de plage et les numéros de partie, voir Utilisation des en-têtes Range et partNumber.
10. (Facultatif) Pour Métriques de demande), choisissez Activer ou Désactiver pour ajouter la surveillance Amazon S3 à votre point d'accès Object Lambda. Les statistiques relatives aux demandes sont facturées au CloudWatch tarif standard d'Amazon.
11. (Facultatif) Sous Object Lambda Access Point policy (Politique de points d'accès Object Lambda), définissez une politique de ressources. Les politiques de ressources accordent des autorisations pour le point d'accès Object Lambda spécifié et peuvent contrôler l'utilisation du point d'accès par ressource, utilisateur ou d'autres conditions. Pour plus d'informations sur les politiques de ressources d'un point d'accès Object Lambda, consultez Configuration des politiques IAM pour les points d'accès Object Lambda.
12. Sous Block Public Access settings for this Object Lambda Access Point (Paramètres de blocage d'accès public pour ce point d'accès Object Lambda), sélectionnez les paramètres de

blocage d'accès public que vous voulez appliquer. Tous les paramètres de blocage d'accès public sont activés par défaut pour les nouveaux points d'accès Object Lambda et nous vous recommandons de laisser les paramètres par défaut activés. Actuellement, Amazon S3 ne prend pas en charge la modification des paramètres de blocage d'accès public d'un point d'accès Object Lambda après la création de ce point d'accès Object Lambda.

Pour plus d'informations sur l'utilisation du blocage de l'accès public Amazon S3, consultez Gestion de l'accès public aux points d'accès pour les compartiments à usage général.

13. Choisissez Create Object Lambda Access Point (Créer un point d'accès Object Lambda).

À l'aide du AWS CLI

Pour créer un point d'accès Object Lambda à l'aide d'un modèle AWS CloudFormation

> **Note**
>
> Pour utiliser les commandes suivantes, remplacez *`user input placeholders`* par vos propres informations.

1. Téléchargez le package de déploiement des AWS Lambda fonctions `s3objectlambda_deployment_package.zip` dans la configuration par défaut de S3 Object Lambda.
2. Exécutez la commande `put-object` suivante pour charger le package dans un compartiment Amazon S3.

```
aws s3api put-object --bucket Amazon S3 bucket name --key
 s3objectlambda_deployment_package.zip --body release/
s3objectlambda_deployment_package.zip
```

3. Téléchargez le AWS CloudFormation modèle dans la `s3objectlambda_defaultconfig.yaml` configuration par défaut de S3 Object Lambda.
4. Exécutez la commande `deploy` suivante pour déployer le modèle dans votre Compte AWS.

```
aws cloudformation deploy --template-file s3objectlambda_defaultconfig.yaml \
 --stack-name AWS CloudFormation stack name \
 --parameter-overrides ObjectLambdaAccessPointName=Object Lambda Access Point name
 \
```

```
 SupportingAccessPointName=Amazon S3 access point S3BucketName=Amazon S3 bucket \
 LambdaFunctionS3BucketName=Amazon S3 bucket containing your Lambda package \
 LambdaFunctionS3Key=Lambda object key LambdaFunctionS3ObjectVersion=Lambda object
version \
 LambdaFunctionRuntime=Lambda function runtime --capabilities capability_IAM
```

Vous pouvez configurer ce AWS CloudFormation modèle pour appeler Lambda pour GETHEAD, et les opérations d'LISTAPI. Pour plus d'informations sur la modification de la configuration par défaut du modèle, consultez the section called "Automatisez la configuration de S3 Object Lambda avec AWS CloudFormation".

Pour créer un point d'accès Object Lambda à l'aide du AWS CLI

> **Note**
>
> Pour utiliser les commandes suivantes, remplacez *user input placeholders* par vos propres informations.

L'exemple suivant crée un point d'accès Object Lambda nommé *my-object-lambda-ap* pour le compartiment *amzn-s3-demo-bucket1* dans le compte *111122223333*. Cet exemple suppose qu'un point d'accès standard nommé *example-ap* a déjà été créé. Pour plus d'informations sur la création d'un point d'accès standard, consultez the section called "Création d'un point d'accès".

Cet exemple utilise la fonction AWS prédéfinie. decompress Pour plus d'informations sur les fonctions prédéfinies, consultez the section called "Utilisation des fonctions AWS intégrées".

1. Créez un compartiment. Dans cet exemple, nous allons utiliser *amzn-s3-demo-bucket1*. Pour plus d'informations sur la création de compartiments, consultez the section called "Création d'un bucket à usage général".
2. Créez un point d'accès standard et attachez-le à votre compartiment. Dans cet exemple, nous allons utiliser *example-ap*. Pour obtenir des informations sur la création de points d'accès standard, consultez the section called "Création d'un point d'accès".
3. Effectuez l'une des actions suivantes :

   - Créez une fonction Lambda dans votre compte que vous souhaitez utiliser pour transformer votre objet Simple Storage Service (Amazon S3). Pour plus d'informations sur la création de fonctions Lambda, consultez the section called "Écriture de fonctions Lambda". Pour utiliser

votre fonction personnalisée avec le AWS CLI, consultez la section Utilisation de Lambda avec le AWS CLI dans le guide du AWS Lambda développeur.

- Utilisez une fonction AWS Lambda prédéfinie. Pour plus d'informations sur les fonctions prédéfinies, consultez Utilisation de AWS fonctions Lambda intégrées.

4. Créez un fichier de configuration JSON nommé `my-olap-configuration.json`. Dans cette configuration, fournissez le point d'accès de prise en charge et l'Amazon Resource Name (ARN) de la fonction Lambda que vous avez créée au cours des étapes précédentes ou l'ARN de la fonction prédéfinie que vous utilisez.

   Example

```
{
    "SupportingAccessPoint" : "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
    "TransformationConfigurations": [{
        "Actions" : ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation" : {
            "AwsLambda": {
                "FunctionPayload" : "{\"compressionType\":\"gzip\"}",
                "FunctionArn" : "arn:aws:lambda:us-east-1:111122223333:function/
compress"
            }
        }
    }]
}
```

5. Exécutez la commande `create-access-point-for-object-lambda` pour créer votre point d'accès Object Lambda.

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-ap --configuration file://my-olap-configuration.json
```

6. (Facultatif) Créez un fichier de stratégie JSON nommé `my-olap-policy.json`.

   L'ajout d'une politique de ressources de points d'accès Object Lambda peut contrôler l'utilisation du point d'accès par ressource, utilisateur ou d'autres conditions. Cette politique de ressources accorde l'autorisation `GetObject` pour le compte *444455556666* au point d'accès Object Lambda spécifié.

Example

```
{
    "Version": "2008-10-17",
    "Statement": [
        {
            "Sid": "Grant account 444455556666 GetObject access",
            "Effect": "Allow",
            "Action": "s3-object-lambda:GetObject",
            "Principal": {
                "AWS": "arn:aws:iam::444455556666:root"
            },
            "Resource": "your-object-lambda-access-point-arn"
        }
    ]
}
```

7. (Facultatif) Exécutez la commande `put-access-point-policy-for-object-lambda` pour définir votre politique de ressources.

```
aws s3control put-access-point-policy-for-object-lambda --account-id 111122223333
 --name my-object-lambda-ap --policy file://my-olap-policy.json
```

8. (Facultatif) Spécifiez une charge utile.

   Une charge utile est un JSON facultatif que vous pouvez fournir à votre AWS Lambda fonction en entrée. Vous pouvez configurer des charges utiles avec différents paramètres pour différents points d'accès Object Lambda qui invoquent la même fonction Lambda, augmentant ainsi la flexibilité de votre fonction Lambda.

   La configuration suivante du point d'accès Object Lambda affiche une charge utile avec deux paramètres.

```
{
 "SupportingAccessPoint": "AccessPointArn",
 "CloudWatchMetricsEnabled": false,
 "TransformationConfigurations": [{
  "Actions": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
  "ContentTransformation": {
   "AwsLambda": {
```

```
    "FunctionArn": "FunctionArn",
    "FunctionPayload": "{\"res-x\": \"100\",\"res-y\": \"100\"}"
   }
  }
 }]
}
```

La configuration de point d'accès Object Lambda suivante montre une charge utile avec un seul paramètre et avec `GetObject-Range`, `GetObject-PartNumber`, `HeadObject-Range` et `HeadObject-PartNumber` activés.

```
{
    "SupportingAccessPoint":"AccessPointArn",
    "CloudWatchMetricsEnabled": false,
    "AllowedFeatures": ["GetObject-Range", "GetObject-PartNumber", "HeadObject-
Range", "HeadObject-PartNumber"],
    "TransformationConfigurations": [{
        "Action": ["GetObject", "HeadObject", "ListObjects", "ListObjectsV2"],
        "ContentTransformation": {
            "AwsLambda": {
                "FunctionArn":"FunctionArn",
                "FunctionPayload": "{\"compression-amount\": \"5\"}"
            }
        }
    }]
}
```

> **Important**
>
> Lorsque vous utilisez des points d'accès Object Lambda, vérifiez que la charge utile ne contient pas d'informations confidentielles.

Utilisation de la AWS CloudFormation console et du modèle

Vous pouvez créer un point d'accès Object Lambda à l'aide de la configuration par défaut fournie par Amazon S3. Vous pouvez télécharger un AWS CloudFormation modèle et le code source d'une fonction Lambda depuis le GitHub référentiel et déployer ces ressources pour configurer un point d'accès Object Lambda fonctionnel.

Pour plus d'informations sur la modification de la configuration par défaut du AWS CloudFormation modèle, consultezthe section called "Automatisez la configuration de S3 Object Lambda avec AWS CloudFormation".

Pour plus d'informations sur la configuration des points d'accès Object Lambda AWS CloudFormation sans le modèle, consultez le guide `AWS::S3ObjectLambda::AccessPoint`de l'AWS CloudFormation utilisateur.

Pour charger le package de déploiement de votre fonction Lambda

1. Téléchargez le package de déploiement des AWS Lambda fonctions `s3objectlambda_deployment_package.zip` dans la configuration par défaut de S3 Object Lambda.
2. Chargez le package dans un compartiment Amazon S3.

Pour créer un point d'accès Object Lambda à l'aide de la console AWS CloudFormation

1. Téléchargez le AWS CloudFormation modèle dans la `s3objectlambda_defaultconfig.yaml` configuration par défaut de S3 Object Lambda.
2. Connectez-vous à la console de AWS gestion et ouvrez la console à l'adresse AWS CloudFormation https://console.aws.amazon.com/cloudformation.
3. Effectuez l'une des actions suivantes :
   - Si vous ne l'avez jamais utilisé AWS CloudFormation auparavant, sur la page d' AWS CloudFormation accueil, choisissez Create stack.
   - Si vous l'avez AWS CloudFormation déjà utilisé, dans le volet de navigation de gauche, choisissez Stacks. Choisissez Create stack (Créer une pile), puis With new resources (standard) (Avec de nouvelles ressources (standard)).
4. Pour Prerequisite - Prepare template (Prérequis – Préparer le modèle), choisissez Template is ready (Le modèle est prêt).
5. Pour Specify template (Spécifier le modèle), choisissez Upload a template file (Charger un fichier de modèle) et chargez `s3objectlambda_defaultconfig.yaml`.
6. Choisissez Next (Suivant).
7. Sur la page Specify stack details (Spécifier les détails de la pile), saisissez un nom pour la pile.
8. Dans la section Parameters (Paramètres), spécifiez les paramètres suivants, définis dans le modèle de pile :

a. Pour CreateNewSupportingAccessPoint, effectuez l'une des actions suivantes :

   - Si vous disposez déjà d'un point d'accès de prise en charge pour le compartiment S3 dans lequel vous avez chargé le modèle, choisissez false (faux).
   - Si vous souhaitez créer un nouveau point d'accès pour ce compartiment, choisissez true (vrai).

b. Pour EnableCloudWatchMonitoring, choisissez vrai ou faux, selon que vous souhaitez activer les métriques de CloudWatch demande et les alarmes Amazon.

c. (Facultatif) Pour LambdaFunctionPayload, ajoutez le texte JSON que vous souhaitez fournir à votre fonction Lambda en entrée. Vous pouvez configurer des charges utiles avec différents paramètres pour différents points d'accès Object Lambda qui invoquent la même fonction Lambda, augmentant ainsi la flexibilité de votre fonction Lambda.

   > **Important**
   >
   > Lorsque vous utilisez des points d'accès Object Lambda, vérifiez que la charge utile ne contient pas d'informations confidentielles.

d. Pour LambdaFunctionRuntime, entrez votre environnement d'exécution préféré pour la fonction Lambda. Les options disponibles sont `nodejs14.x`, `python3.9` et `java11`.

e. Pour LambdaFunctionS3 BucketName, entrez le nom du compartiment Amazon S3 dans lequel vous avez chargé le package de déploiement.

f. Pour LambdaFunctionS3Key, entrez la clé d'objet Amazon S3 sur laquelle vous avez chargé le package de déploiement.

g. Pour LambdaFunctionS3 ObjectVersion, entrez la version de l'objet Amazon S3 dans laquelle vous avez chargé le package de déploiement.

h. Pour ObjectLambdaAccessPointName, entrez un nom pour votre point d'accès Object Lambda.

i. Pour S3 BucketName, entrez le nom du compartiment Amazon S3 qui sera associé à votre point d'accès Object Lambda.

j. Pour SupportingAccessPointName, entrez le nom de votre point d'accès compatible.

> **Note**
>
> Il s'agit d'un point d'accès associé au compartiment Amazon S3 que vous avez choisi à l'étape précédente. Si aucun point d'accès n'est associé à votre compartiment Amazon S3, vous pouvez configurer le modèle pour en créer un pour vous en choisissant true for CreateNewSupportingAccessPoint.

9. Choisissez Next (Suivant).
10. Sur la page Configurer les options de pile, choisissez Suivant.

    Pour plus d'informations sur les paramètres facultatifs figurant sur cette page, consultez Définition des options des piles AWS CloudFormation dans le Guide de l'utilisateur AWS CloudFormation .
11. Sur la page Review (Vérification), choisissez Create stack (Créer une pile).

À l'aide du AWS Cloud Development Kit (AWS CDK)

Pour plus d'informations sur la configuration des points d'accès Object Lambda à l'aide de AWS CDK, consultez la section `AWS::S3ObjectLambda`Construct Library dans la référence de l'AWS Cloud Development Kit (AWS CDK) API.

Automatisez la configuration de S3 Object Lambda à l'aide d'un modèle CloudFormation

Vous pouvez utiliser un AWS CloudFormation modèle pour créer rapidement un point d'accès Amazon S3 Object Lambda. Le CloudFormation modèle crée automatiquement les ressources pertinentes, configure les rôles AWS Identity and Access Management (IAM) et met en place une AWS Lambda fonction qui gère automatiquement les demandes via le point d'accès Object Lambda. Ce CloudFormation modèle vous permet de mettre en œuvre les meilleures pratiques, d'améliorer votre niveau de sécurité et de réduire les erreurs causées par les processus manuels.

Ce GitHub référentiel contient le CloudFormation modèle et le code source de la fonction Lambda. Pour obtenir des instructions sur l'utilisation de ce modèle, consultez the section called "Création de points d'accès Object Lambda".

La fonction Lambda fournie dans ce modèle n'exécute aucune transformation. Au lieu de cela, il renvoie vos objets tels quels à partir de la source de données sous-jacente. Vous pouvez cloner la fonction et ajouter votre propre code de transformation pour modifier et traiter les données

lorsqu'elles sont renvoyées vers une application. Pour plus d'informations sur la modification de votre fonction, consultez the section called "Modification de la fonction Lambda" et the section called "Écriture de fonctions Lambda".

Modification du modèle.

Création d'un nouveau point d'accès de prise en charge

S3 Object Lambda utilise deux points d'accès, un point d'accès Object Lambda et un point d'accès S3 standard, appelé point d'accès de prise en charge. Lorsque vous effectuez une demande auprès d'un point d'accès Object Lambda, S3 invoque Lambda en votre nom ou délègue la demande au point d'accès de prise en charge, en fonction de la configuration S3 Object Lambda. Vous pouvez créer un nouveau point d'accès de prise en charge en transmettant le paramètre suivant dans le cadre de la commande `aws cloudformation deploy` lors du déploiement du modèle.

```
CreateNewSupportingAccessPoint=true
```

Configuration d'une charge utile de fonction

Vous pouvez configurer une charge utile de manière à fournir des données supplémentaires à la fonction Lambda en transmettant le paramètre suivant dans le cadre de la commande `aws cloudformation deploy` lors du déploiement du modèle.

```
LambdaFunctionPayload="format=json"
```

Activation de la CloudWatch surveillance d'Amazon

Vous pouvez activer la CloudWatch surveillance en transmettant le paramètre suivant dans le cadre de la `aws cloudformation deploy` commande lors du déploiement du modèle.

```
EnableCloudWatchMonitoring=true
```

Ce paramètre active votre point d'accès Object Lambda pour les métriques de demande Amazon S3 et crée deux CloudWatch alarmes pour surveiller les erreurs côté client et côté serveur.

> **Note**
>
> CloudWatch L'utilisation d'Amazon entraînera des coûts supplémentaires. Pour plus d'informations sur les métriques de demande Amazon S3, consultez Surveillance et journalisation des points d'accès.

Pour plus d'informations sur la tarification, consultez Tarification CloudWatch .

Configuration de la simultanéité provisionnée

Pour réduire la latence, vous pouvez configurer la simultanéité provisionnée pour la fonction Lambda qui soutient le point d'accès Object Lambda, en modifiant le modèle afin d'inclure les lignes suivantes sous `Resources`.

```
LambdaFunctionVersion:
      Type: AWS::Lambda::Version
      Properties:
        FunctionName: !Ref LambdaFunction
        ProvisionedConcurrencyConfig:
            ProvisionedConcurrentExecutions: Integer
```

> **Note**
>
> Des frais supplémentaires pour le provisionnement simultané vous seront facturés. Pour plus d'informations sur la simultanéité provisionnée, consultez Gestion de la simultanéité provisionnée Lambda dans le Guide du développeur AWS Lambda .
> Pour plus d'informations sur la tarification, consultez Tarification AWS Lambda.

Modification de la fonction Lambda

Modification des valeurs d'en-tête d'une requête **`GetObject`**

Par défaut, la fonction Lambda transfère tous les en-têtes, à l'exception de `Content-Length` et `ETag`, de la demande d'URL pré-signée au client `GetObject`. En fonction de votre code de transformation dans la fonction Lambda, vous pouvez choisir d'envoyer de nouvelles valeurs d'en-tête à la demande `GetObject` du client.

Vous pouvez mettre à jour votre fonction Lambda pour envoyer de nouvelles valeurs d'en-tête en les transmettant dans l'opération d'API `WriteGetObjectResponse`.

Par exemple, si votre fonction Lambda traduit du texte dans des objets Amazon S3 vers une autre langue, vous pouvez transmettre une nouvelle valeur dans l'en-tête `Content-Language`. Pour ce faire, vous pouvez modifier la fonction `writeResponse` comme suit :

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
    },
    ...headers,
    ContentLanguage: 'my-new-language'
  }).promise();
}
```

Pour obtenir la liste complète des en-têtes pris en charge, consultez `WriteGetObjectResponse` dans la Référence d'API Amazon Simple Storage Service.

Renvoi des en-têtes de métadonnées

Vous pouvez mettre à jour votre fonction Lambda pour envoyer de nouvelles valeurs d'en-tête en les transmettant dans la demande d'opération d'API `WriteGetObjectResponse`.

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest,
      'my-new-header': 'my-new-value'
    },
    ...headers
  }).promise();
```

```
}
```

Renvoi d'un nouveau code de statut

Vous pouvez renvoyer un code de statut personnalisé au client `GetObject` en transmettant ce code dans la demande d'opération d'API `WriteGetObjectResponse`.

```
async function writeResponse (s3Client: S3, requestContext: GetObjectContext,
 transformedObject: Buffer,
  headers: Headers): Promise<PromiseResult<{}, AWSError>> {
  const { algorithm, digest } = getChecksum(transformedObject);

  return s3Client.writeGetObjectResponse({
    RequestRoute: requestContext.outputRoute,
    RequestToken: requestContext.outputToken,
    Body: transformedObject,
    Metadata: {
      'body-checksum-algorithm': algorithm,
      'body-checksum-digest': digest
    },
    ...headers,
    StatusCode: Integer
  }).promise();
}
```

Pour obtenir la liste complète des codes de statut pris en charge, consultez `WriteGetObjectResponse` dans la Référence d'API Amazon Simple Storage Service.

Application des paramètres **`Range`** et **`partNumber`** à l'objet source

Par défaut, le point d'accès Object Lambda créé par le CloudFormation modèle peut gérer les paramètres `Range` et`partNumber`. La fonction Lambda applique la plage ou le numéro de partie demandé à l'objet transformé. Pour ce faire, la fonction doit télécharger l'objet entier et exécuter la transformation. Dans certains cas, vos plages d'objets transformés peuvent correspondre exactement à vos plages d'objets source. Cela signifie que la demande de plage d'octets A-B sur votre objet source et l'exécution de la transformation peuvent fournir le même résultat que la demande de l'objet entier, l'exécution de la transformation et le renvoi de la plage d'octets A-B sur l'objet transformé.

Dans ce cas, vous pouvez modifier l'implémentation de la fonction Lambda pour appliquer la plage ou le numéro de partie directement à l'objet source. Cette approche réduit la latence globale de

la fonction ainsi que la mémoire requise. Pour plus d'informations, consultez the section called "Utilisation des en-têtes Range et partNumber".

Désactivation de la gestion de **`Range`** et **`partNumber`**

Par défaut, le point d'accès Object Lambda créé par le CloudFormation modèle peut gérer les paramètres `Range` et`partNumber`. Si vous n'avez pas besoin de ce comportement, vous pouvez le désactiver en supprimant les lignes suivantes du modèle :

```
AllowedFeatures:
  - GetObject-Range
  - GetObject-PartNumber
  - HeadObject-Range
  - HeadObject-PartNumber
```

Transformation de large objets

Par défaut, la fonction Lambda traite l'ensemble de l'objet en mémoire avant de pouvoir commencer à diffuser la réponse vers S3 Object Lambda. Vous pouvez modifier la fonction pour diffuser la réponse au fur et à mesure qu'elle effectue la transformation. Cela permet de réduire la latence de transformation et la mémoire de la fonction Lambda. Pour obtenir un exemple de mise en œuvre, consultez Stream compressed content example (Exemple de diffusion de contenu compressé).

Utilisation des points d'accès Amazon S3 Object Lambda

Les demandes via des points d'accès Amazon S3 Object Lambda fonctionnent de la même manière que les demandes via d'autres points d'accès. Pour plus d'informations sur les demandes via un point d'accès, consultez Utilisation des points d'accès Amazon S3 pour des compartiments à usage général. Vous pouvez effectuer des demandes via les points d'accès Object Lambda à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) ou de l' AWS SDKsAPI REST Amazon S3.

> **Important**
>
> Les Amazon Resource Names (ARNs) pour les points d'accès Object Lambda utilisent le nom de service. `s3-object-lambda` Ainsi, le point d'accès Object Lambda ARNs commence par`arn:aws::s3-object-lambda`, au lieu de`arn:aws::s3`, par celui qui est utilisé avec d'autres points d'accès.

Comment trouver l'ARN de votre point d'accès Object Lambda

Pour utiliser un point d'accès Object Lambda avec le AWS CLI ou AWS SDKs, vous devez connaître le nom de ressource Amazon (ARN) du point d'accès Object Lambda. Les exemples suivants montrent comment trouver l'ARN d'un point d'accès Object Lambda à l'aide de la console Amazon S3 ou de l' AWS CLI.

Utilisation de la console S3

Pour trouver l'ARN de votre point d'accès Object Lambda avec la console

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Sélectionnez le bouton d'option en regard du point d'accès Object Lambda dont vous souhaitez copier l'ARN.
4. Choisissez Copier l'ARN.

À l'aide du AWS CLI

Pour trouver l'ARN de votre point d'accès Object Lambda à l'aide du AWS CLI

1. Pour récupérer la liste des points d'accès Object Lambda associés à votre Compte AWS, exécutez la commande suivante. Avant d'exécuter la commande, remplacez l'identifiant du compte *111122223333* par le Compte AWS vôtre.

```
aws s3control list-access-points-for-object-lambda --account-id 111122223333
```

2. Lisez la sortie de la commande pour trouver l'ARN du point d'accès Object Lambda que vous souhaitez utiliser. La sortie de la commande précédente doit ressembler à celle de l'exemple suivant.

```
{
    "ObjectLambdaAccessPointList": [
        {
            "Name": "my-object-lambda-ap",
            "ObjectLambdaAccessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/my-object-lambda-ap"
        },
```

```
        ...
    ]
}
```

Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda de compartiment S3

Quand vous créez un point d'accès Object Lambda, Amazon S3 génère automatiquement un alias unique pour votre point d'accès Object Lambda. Vous pouvez utiliser cet alias à la place d'un nom de compartiment Amazon S3 ou de l'Amazon Resource Name (ARN) du point d'accès Object Lambda dans une demande pour les opérations de plan de données de point d'accès. Pour obtenir la liste de ces opérations, consultez la page Compatibilité avec les points d'accès.

Un nom d'alias de point d'accès Object Lambda est créé dans le même espace de noms qu'un compartiment Amazon S3. Ce nom d'alias est généré automatiquement et ne peut pas être modifié. Pour un point d'accès Object Lambda existant, un alias est automatiquement attribué. Un nom d'alias de point d'accès Object Lambda répond à toutes les exigences d'un nom de compartiment Amazon S3 valide et comprend les parties suivantes :

Object Lambda Access Point name prefix-*metadata*--ol-s3

> **Note**
>
> Le suffixe `--ol-s3` est réservé aux noms d'alias de point d'accès Object Lambda et ne peut pas être utilisé pour les noms de compartiment ou de point d'accès Object Lambda. Pour plus d'informations sur les règles d'attribution de noms des compartiments Amazon S3, consultez Règles de dénomination des compartiments à usage général.

Voici des exemples d'ARN et d'alias de point d'accès Object Lambda pour un point d'accès Object Lambda nommé *my-object-lambda-access-point* :

- ARN – arn:aws:s3-object-lambda:*region*:*account-id*:accesspoint/*my-object-lambda-access-point*
- Alias de point d'accès Object Lambda : *my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a*--ol-s3

Lorsque vous utilisez un point d'accès Object Lambda, vous pouvez utiliser le nom d'alias du point d'accès Object Lambda sans d'importantes modifications de code.

Lorsque vous supprimez un point d'accès Object Lambda, le nom d'alias du point d'accès Object Lambda devient inactif et n'est plus provisionné.

Comment trouver l'alias de votre point d'accès Object Lambda

Utilisation de la console S3

Pour trouver l'alias de votre point d'accès Object Lambda avec la console

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Pour le point d'accès Object Lambda que vous souhaitez utiliser, copiez la valeur de l'alias du point d'accès Object Lambda.

À l'aide du AWS CLI

Lorsque vous créez un point d'accès Object Lambda, Amazon S3 génère automatiquement un nom d'alias de point d'accès Object Lambda, comme illustré dans l'exemple de commande suivant. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations. Pour plus d'informations sur la création d'un point d'accès Object Lambda à l'aide du AWS CLI, consultez. Pour créer un point d'accès Object Lambda à l'aide du AWS CLI

```
aws s3control create-access-point-for-object-lambda --account-id 111122223333 --
name my-object-lambda-access-point --configuration file://my-olap-configuration.json
{
    "ObjectLambdaAccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-
access-point",
    "Alias": {
        "Value": "my-object-lambda-acc-1a4n8yjrb3kda96f67zwrwiiuse1a--ol-s3",
        "Status": "READY"
    }
}
```

Le nom d'alias du point d'accès Object Lambda généré comporte deux champs :

- Le champ `Value` est la valeur d'alias du point d'accès Object Lambda.

- Le champ `Status` est le statut de l'alias du point d'accès Object Lambda. Si le statut est `PROVISIONING`, Amazon S3 fournit l'alias du point d'accès Object Lambda, qui n'est pas encore prêt à être utilisé. Si le statut est `READY`, l'alias du point d'accès Object Lambda a été correctement provisionné et est prêt à être utilisé.

Pour plus d'informations sur le type de données `ObjectLambdaAccessPointAlias` dans l'API REST, consultez CreateAccessPointForObjectLambda et ObjectLambdaAccessPointAlias dans la Référence d'API Amazon Simple Storage Service.

Comment utiliser l'alias du point d'accès Object Lambda

Vous pouvez utiliser un alias de point d'accès Object Lambda plutôt qu'un nom de compartiment Amazon S3 pour les opérations répertoriées dans Compatibilité avec les points d'accès.

L' AWS CLI exemple de `get-bucket-location` commande suivant utilise l'alias du point d'accès du compartiment pour renvoyer le nom dans Région AWS lequel se trouve le compartiment. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api get-bucket-location --bucket my-object-lambda-
acc-w7i37nq6xuzgax3jw3oqtifiusw2a--ol-s3

{
    "LocationConstraint": "us-west-2"
}
```

Si l'alias du point d'accès Object Lambda indiqué dans une demande n'est pas valide, le code d'erreur `InvalidAccessPointAliasError` est renvoyé. Pour plus d'informations sur `InvalidAccessPointAliasError`, consultez List of Error Codes dans la Référence d'API Amazon Simple Storage Service.

Les limites d'un alias de point d'accès Object Lambda sont les mêmes que celles d'un alias de point d'accès. Pour plus d'informations sur les limites d'un alias de point d'accès, consultez Limitations relatives aux alias des points d'accès.

Considérations sur la sécurité pour les points d'accès S3 Object Lambda

Avec Amazon S3 Object Lambda, vous pouvez effectuer des transformations personnalisées sur les données lorsqu'elles quittent Amazon S3 en utilisant l'évolutivité et la flexibilité d'une AWS Lambda plate-forme de calcul. S3 et Lambda restent sécurisés par défaut, mais une attention

particulière de l'auteur de fonction Lambda est nécessaire pour maintenir cette sécurité. S3 Object Lambda nécessite que tous les accès soient effectués par des mandataires authentifiés (pas d'accès anonyme) et via HTTPS.

Pour limiter les risques de sécurité, nous vous recommandons de respecter les points suivants :

- Étendez le rôle d'exécution Lambda au plus petit ensemble d'autorisations possible.
- Dans la mesure du possible, veillez à ce que votre fonction Lambda accède à Amazon S3 via l'URL pré-signée fournie.

Configuration des politiques IAM

Les points d'accès S3 prennent en charge les politiques de ressources AWS Identity and Access Management (IAM) qui vous permettent de contrôler l'utilisation du point d'accès par ressource, par utilisateur ou selon d'autres conditions. Pour de plus amples informations, veuillez consulter Configuration des politiques IAM pour les points d'accès Object Lambda.

Comportement de chiffrement

Étant donné que les points d'accès Object Lambda utilisent à la fois Amazon S3 et qu' AWS Lambda il existe des différences de comportement de chiffrement. Pour plus d'informations sur le comportement de chiffrement S3 par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.

- Lorsque vous utilisez le chiffrement côté serveur S3 avec des points d'accès Object Lambda, l'objet est déchiffré avant d'être envoyé à Lambda. Une fois l'objet envoyé à Lambda, il est traité sous sa forme déchiffrée (dans le cas d'une requête `GET` ou `HEAD`).
- Pour empêcher la journalisation de la clé de chiffrement, S3 rejette les requêtes `GET` et `HEAD` pour les objets chiffrés côté serveur avec des clés fournies par le client (SSE-C). Toutefois, la fonction Lambda peut encore récupérer ces objets si elle a accès à la clé fournie par le client.
- Lorsque vous utilisez le chiffrement côté client S3 avec des points d'accès Object Lambda, veillez à ce que Lambda ait accès à la clé de chiffrement pour pouvoir déchiffrer et rechiffrer l'objet.

Sécurité des points d'accès

S3 Object Lambda utilise deux points d'accès, un point d'accès Object Lambda et un point d'accès S3 standard, appelé point d'accès de prise en charge. Lorsque vous effectuez une demande auprès

d'un point d'accès Object Lambda, S3 appelle Lambda en votre nom ou délègue la demande au point d'accès de prise en charge, en fonction de la configuration S3 Object Lambda. Lorsque Lambda est invoqué pour une demande, S3 génère une URL pré-signée sur votre objet en votre nom via le point d'accès de prise en charge. Votre fonction Lambda reçoit cette URL en entrée quand la fonction est invoquée.

Vous pouvez définir votre fonction Lambda pour utiliser cette URL pré-signée pour récupérer l'objet d'origine, au lieu d'invoquer S3 directement. Ce modèle vous permet d'appliquer de meilleures limites de sécurité à vos objets. Vous pouvez limiter l'accès direct des objets à un ensemble limité de rôles ou d'utilisateurs IAM par le biais de compartiments S3 ou de points d'accès S3. Cette approche protège également vos fonctions Lambda face au problème de l'adjoint confus, dans le cadre duquel une fonction mal configurée, dotée d'autorisations différentes de l'appelant, pourrait autoriser ou refuser l'accès aux objets alors qu'elle ne le devrait pas.

Accès public au point d'accès Object Lambda

S3 Object Lambda n'autorise pas un accès anonyme ou public, car Amazon S3 doit autoriser votre identité pour effectuer une demande S3 Object Lambda quelconque. Lorsque vous invoquez des demandes via un point d'accès Object Lambda, vous devez avoir l'autorisation `lambda:InvokeFunction` pour la fonction Lambda configurée. De même, lorsque vous invoquez d'autres opérations d'API via un point d'accès Object Lambda, vous devez disposer des autorisations `s3:*` requises.

Sans ces autorisations, les demandes d'invocation de Lambda et de délégation à S3 échouent avec des erreurs HTTP 403 (Interdit). Tous les accès doivent être effectués par des mandants authentifiés. Si vous avez besoin d'un accès public, vous pouvez utiliser Lambda@Edge comme alternative. Pour plus d'informations, consultez la section Personnalisation en périphérie avec Lambda @Edge dans le manuel CloudFront Amazon Developer Guide.

Adresses IP des points d'accès Object Lambda

Les sous-réseaux `describe-managed-prefix-lists` prennent en charge les points de terminaison de cloud privé virtuel (VPC) de la passerelle et sont liés à la table de routage des points de terminaison du VPC. Comme le point d'accès Object Lambda ne prend pas en charge le VPC de passerelle, ses plages IP sont manquantes. Les plages manquantes appartiennent à Amazon S3, mais ne sont pas prises en charge par les points de terminaison de VPC de la passerelle. Pour plus d'informations`describe-managed-prefix-lists`, consultez DescribeManagedPrefixListsla référence des EC2 API Amazon et les plages d'adresses AWS IP dans le Références générales AWS.

Configuration des politiques IAM pour les points d'accès Object Lambda

Les points d'accès Amazon S3 prennent en charge les politiques de ressources AWS Identity and Access Management (IAM) que vous pouvez utiliser pour contrôler l'utilisation du point d'accès par ressource, par utilisateur ou selon d'autres conditions. Vous pouvez contrôler l'accès par le biais d'une politique de ressources facultative sur votre point d'accès Object Lambda ou d'une politique de ressources sur le point d'accès de prise en charge. Pour step-by-step des exemples, voir Didacticiel : Transformation de données pour votre application avec S3 Object Lambda etDidacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend.

Les quatre ressources suivantes doivent disposer d'autorisations pour utiliser les points d'accès Object Lambda :

- L'identité IAM, telle que l'utilisateur ou le rôle. Pour obtenir plus d'informations sur les identités IAM et sur les bonnes pratiques, consultez Identités IAM (utilisateurs, groupes d'utilisateurs et rôles) dans le Guide de l'utilisateur IAM.
- Point d'accès standard connecté à une source de données sous-jacente telle qu'un compartiment S3 ou un volume Amazon FSx pour OpenZFS. Lorsque vous utilisez des points d'accès Object Lambda, ce point d'accès standard est appelé point d'accès de prise en charge.
- Le point d'accès Object Lambda.
- La AWS Lambda fonction.

> **Important**
>
> Avant d'enregistrer votre politique, assurez-vous de résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions de AWS Identity and Access Management Access Analyzer. IAM Access Analyzer exécute des vérifications de politiques pour valider votre politique par rapport à la grammaire de politique et aux bonnes pratiques IAM. Ces vérifications génèrent des résultats et fournissent des recommandations exploitables pour vous aider à créer des stratégies fonctionnelles et conformes aux bonnes pratiques en matière de sécurité.
>
> Pour en savoir plus sur la validation des politiques à l'aide d'IAM Access Analyzer, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM. Pour afficher la liste des avertissements, erreurs et suggestions renvoyés par IAM Access Analyzer, consultez la Référence de vérification de politique IAM Access Analyzer.

Les exemples de politique suivants supposent que vous disposez des ressources suivantes :

- Un compartiment Amazon S3 avec l'Amazon Resource Name (ARN) suivant :

  `arn:aws:s3:::amzn-s3-demo-bucket1`

- Un point d'accès Amazon S3 Standard sur ce compartiment avec l'ARN suivant :

  `arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point`

- Un point d'accès Object Lambda avec l'ARN suivant :

  `arn:aws:s3-object-lambda:us-east-1:111122223333:accesspoint/my-object-lambda-ap`

- Une AWS Lambda fonction avec l'ARN suivant :

  `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction`

> **Note**
>
> Si vous utilisez une fonction Lambda de votre compte, vous devez inclure la version de cette fonction dans votre déclaration de politique. Dans l'exemple d'ARN suivant, la version est indiquée par *1* :
> `arn:aws:lambda:us-east-1:111122223333:function:MyObjectLambdaFunction:1`
> Lambda ne prend pas en charge l'ajout de politiques IAM à la version $LATEST. Pour plus d'informations sur les versions des fonctions Lambda, consultez Versions de fonctions Lambda dans le Guide du développeur AWS Lambda .

Example – Politique de compartiment qui délègue le contrôle d'accès aux points d'accès standard

L'exemple de politique de compartiment S3 suivant délègue le contrôle d'accès pour un compartiment aux points d'accès standard du compartiment. Cette politique permet un accès complet à tous les points d'accès appartenant au compte du propriétaire du compartiment. Ainsi, tous les accès à ce compartiment sont contrôlés par les politiques attachées à ses points d'accès. Les utilisateurs peuvent lire à partir du compartiment uniquement via un point d'accès, ce qui signifie que les opérations peuvent uniquement être invoquées via des points d'accès. Pour de plus amples informations, veuillez consulter Délégation du contrôle d'accès aux points d'accès.

JSON

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS":"account-ARN"},
        "Action" : "*",
        "Resource" : [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Bucket owner's
 account ID" }
        }
    }]
}
```

Example : politique IAM qui accorde à un utilisateur les autorisations nécessaires pour utiliser un point d'accès Object Lambda

La politique IAM suivante accorde à un utilisateur des autorisations sur la fonction Lambda, le point d'accès standard et le point d'accès Object Lambda.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowLambdaInvocation",
      "Action": [
        "lambda:InvokeFunction"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:MyObjectLambdaFunction:1",
      "Condition": {
```

```
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowStandardAccessPointAccess",
      "Action": [
        "s3:Get*",
        "s3:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point/
*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "s3-object-lambda.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid": "AllowObjectLambdaAccess",
      "Action": [
        "s3-object-lambda:Get*",
        "s3-object-lambda:List*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/my-object-lambda-ap"
    }
  ]
}
```

Activation des autorisations pour les rôles d'exécution Lambda

Quand des demandes `GET` sont adressées à un point d'accès Object Lambda, votre fonction Lambda a besoin d'une autorisation pour envoyer les données au point d'accès S3 Object Lambda. Cette autorisation est fournie en activant l'autorisation `s3-object-lambda:WriteGetObjectResponse`

sur le rôle d'exécution de votre fonction Lambda. Vous pouvez créer un rôle d'exécution ou mettre à jour un rôle existant.

> **Note**
>
> Votre fonction a besoin de l'autorisation `s3-object-lambda:WriteGetObjectResponse` uniquement si vous réalisez une requête `GET`.

Pour créer un rôle d'exécution dans la console IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, choisissez Rôles.
3. Choisissez Créer un rôle.
4. Sous Cas d'utilisation courants, choisissez Lambda.
5. Choisissez Suivant.
6. Sur la page Ajouter des autorisations, recherchez la stratégie AWS gérée `AmazonS3ObjectLambdaExecutionRolePolicy`, puis cochez la case à côté du nom de la stratégie.

   Cette politique doit contenir l'action `s3-object-lambda:WriteGetObjectResponse`.
7. Choisissez Suivant.
8. Sur la page Name, review, and create (Nommer, vérifier et créer), pour Role name (Nom du rôle), saisissez **`s3-object-lambda-role`**.
9. (Facultatif) Ajoutez une description et des balises pour ce rôle.
10. Choisissez Créer un rôle.
11. Appliquez l'objet récemment créé **`s3-object-lambda-role`** comme rôle d'exécution de votre fonction Lambda. Cela peut être fait pendant ou après la création de la fonction Lambda dans la console Lambda.

Pour plus d'informations sur les rôles d'exécution, consultez Rôle d'exécution Lambda dans le Guide du développeur AWS Lambda .

Utilisation des clés de contexte avec des points d'accès Object Lambda

S3 Object Lambda évaluera les clés de contexte telles que `s3-object-lambda:TlsVersion` ou `s3-object-lambda:AuthType` qui sont liées à la connexion ou à la signature de la demande. Toutes les autres clés de contexte, telles que `s3:prefix`, sont évaluées par Simple Storage Service (Amazon S3).

Prise en charge du CORS du point d'accès Object Lambda

Quand S3 Object Lambda reçoit une demande d'un navigateur ou que la demande inclut un en-tête `Origin`, S3 Object Lambda ajoute toujours un champ d'en-tête `"AllowedOrigins":"*"`.

Pour plus d'informations, consultez Utilisation du partage des ressources entre origines multiples (CORS).

Écriture de fonctions Lambda pour les points d'accès S3 Object Lambda

Cette section explique comment écrire des AWS Lambda fonctions à utiliser avec les points d'accès Amazon S3 Object Lambda.

Pour en savoir plus sur end-to-end les procédures complètes relatives à certaines tâches S3 Object Lambda, consultez les rubriques suivantes :

- Didacticiel : Transformation de données pour votre application avec S3 Object Lambda
- Didacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend
- Tutoriel : Utilisation de S3 Object Lambda pour filigraner dynamiquement des images au fur et à mesure de leur récupération

Rubriques

- Utilisation de requêtes GetObject dans Lambda
- Utilisation de requêtes HeadObject dans Lambda
- Utilisation de requêtes ListObjects dans Lambda
- Utilisation de requêtes ListObjectsV2 dans Lambda
- Format et utilisation du contexte d'événement
- Utilisation des en-têtes Range et partNumber

Utilisation de requêtes **`GetObject`** dans Lambda

Cette section suppose que votre point d'accès Object Lambda est configuré pour appeler la fonction Lambda pour `GetObject`. S3 Object Lambda inclut l'opération d'API Amazon S3, `WriteGetObjectResponse`, qui permet à la fonction Lambda de fournir des données personnalisées et des en-têtes de réponse à l'appelant `GetObject`.

`WriteGetObjectResponse` vous offre un contrôle étendu sur le code de statut, les en-têtes de réponse et le corps de réponse, en fonction de vos besoins de traitement. Vous pouvez utiliser `WriteGetObjectResponse` pour répondre avec l'ensemble de l'objet transformé, des parties de l'objet transformé ou d'autres réponses basées sur le contexte de votre application. La section suivante présente des exemples uniques d'utilisation de l'opération d'API `WriteGetObjectResponse`.

- Exemple 1 : répondre avec un code de statut HTTP 403 (Interdit)
- Exemple 2 : répondre avec une image transformée
- Exemple 3 : diffuser du contenu compressé

Exemple 1 : répondre avec un code de statut HTTP 403 (Interdit)

Vous pouvez utiliser `WriteGetObjectResponse` pour répondre avec le code d'état HTTP 403 (Interdit) en fonction du contenu de l'objet.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import java.io.ByteArrayInputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example1 {
```

```
    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();

        // Check to see if the request contains all of the necessary information.
        // If it does not, send a 4XX response and a custom error code and message.
        // Otherwise, retrieve the object from S3 and stream it
        // to the client unchanged.
        var tokenIsNotPresent = !
event.getUserRequest().getHeaders().containsKey("requiredToken");
        if (tokenIsNotPresent) {
            s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                    .withRequestRoute(event.outputRoute())
                    .withRequestToken(event.outputToken())
                    .withStatusCode(403)
                    .withContentLength(0L).withInputStream(new
 ByteArrayInputStream(new byte[0]))
                    .withErrorCode("MissingRequiredToken")
                    .withErrorMessage("The required token was not present in the
 request."));
            return;
        }

        // Prepare the presigned URL for use and make the request to S3.
        HttpClient httpClient = HttpClient.newBuilder().build();
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Stream the original bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(presignedResponse.body()));
    }
}
```

Python

```
import boto3
import requests
```

```
def handler(event, context):
    s3 = boto3.client('s3')

    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and contains a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to
    S3 Object Lambda.
    """
    get_context = event["getObjectContext"]
    user_request_headers = event["userRequest"]["headers"]

    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    # Check for the presence of a 'CustomHeader' header and deny or allow based on
 that header.
    is_token_present = "SuperSecretToken" in user_request_headers

    if is_token_present:
        # If the user presented our custom 'SuperSecretToken' header, we send the
 requested object back to the user.
        response = requests.get(s3_url)
        s3.write_get_object_response(RequestRoute=route, RequestToken=token,
 Body=response.content)
    else:
        # If the token is not present, we send an error back to the user.
        s3.write_get_object_response(RequestRoute=route, RequestToken=token,
 StatusCode=403,
        ErrorCode="NoSuperSecretTokenFound", ErrorMessage="The request was not
 secret enough.")

    # Gracefully exit the Lambda function.
    return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
```

```
exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and contains a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    // The 'userRequest' object has information related to the user who made this
 'GetObject' request to S3 Object Lambda.
    const { userRequest, getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Check for the presence of a 'CustomHeader' header and deny or allow based on
 that header.
    const isTokenPresent = Object
        .keys(userRequest.headers)
        .includes("SuperSecretToken");

    if (!isTokenPresent) {
        // If the token is not present, we send an error back to the user. The
 'await' in front of the request
        // indicates that we want to wait for this request to finish sending before
 moving on.
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            StatusCode: 403,
            ErrorCode: "NoSuperSecretTokenFound",
            ErrorMessage: "The request was not secret enough.",
        }).promise();
    } else {
        // If the user presented our custom 'SuperSecretToken' header, we send the
 requested object back to the user.
        // Again, note the presence of 'await'.
        const presignedResponse = await axios.get(inputS3Url);
        await s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            Body: presignedResponse.data,
        }).promise();
    }

    // Gracefully exit the Lambda function.
```

```
    return { statusCode: 200 };
}
```

Exemple 2 : répondre avec une image transformée

Lorsque vous effectuez une transformation d'image, vous pouvez constater que vous avez besoin de tous les octets de l'objet source avant de pouvoir commencer à les traiter. Dans ce cas, votre demande `WriteGetObjectResponse` renvoie l'objet entier à l'application requérante en un seul appel.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import javax.imageio.ImageIO;
import java.awt.image.BufferedImage;
import java.awt.Image;
import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;

public class Example2 {

    private static final int HEIGHT = 250;
    private static final int WIDTH = 250;

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Prepare the presigned URL for use and make the request to S3.
```

```
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // The entire image is loaded into memory here so that we can resize it.
        // Once the resizing is completed, we write the bytes into the body
        // of the WriteGetObjectResponse request.
        var originalImage = ImageIO.read(presignedResponse.body());
        var resizingImage = originalImage.getScaledInstance(WIDTH, HEIGHT,
 Image.SCALE_DEFAULT);
        var resizedImage = new BufferedImage(WIDTH, HEIGHT,
 BufferedImage.TYPE_INT_RGB);
        resizedImage.createGraphics().drawImage(resizingImage, 0, 0, WIDTH, HEIGHT,
 null);

        var baos = new ByteArrayOutputStream();
        ImageIO.write(resizedImage, "png", baos);

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(new ByteArrayInputStream(baos.toByteArray())));
    }
}
```

Python

```
import boto3
import requests
import io
from PIL import Image

def handler(event, context):
    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to
    S3 Object Lambda.
    """
```

```
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    """
    In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
    'inputS3Url'.
    """
    image_request = requests.get(s3_url)
    image = Image.open(io.BytesIO(image_request.content))
    image.thumbnail((256,256), Image.ANTIALIAS)

    transformed = io.BytesIO()
    image.save(transformed, "png")

    # Send the resized image back to the client.
    s3 = boto3.client('s3')
    s3.write_get_object_response(Body=transformed.getvalue(), RequestRoute=route,
 RequestToken=token)

    # Gracefully exit the Lambda function.
    return { 'status_code': 200 }
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const sharp = require('sharp');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // In this case, we're resizing .png images that are stored in S3 and are
 accessible through the presigned URL
```

```
    // 'inputS3Url'.
    const { data } = await axios.get(inputS3Url, { responseType: 'arraybuffer' });

    // Resize the image.
    const resized = await sharp(data)
        .resize({ width: 256, height: 256 })
        .toBuffer();

    // Send the resized image back to the client.
    await s3.writeGetObjectResponse({
        RequestRoute: outputRoute,
        RequestToken: outputToken,
        Body: resized,
    }).promise();

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

Exemple 3 : diffuser du contenu compressé

Lorsque vous compressez des objets, les données compressées sont produites de manière incrémentielle. Par conséquent, vous pouvez utiliser votre demande `WriteGetObjectResponse` pour renvoyer les données compressées dès qu'elles sont prêtes. Comme le montre cet exemple, vous n'avez pas besoin de connaître la longueur de la transformation terminée.

Java

```
package com.amazon.s3.objectlambda;

import com.amazonaws.services.lambda.runtime.events.S3ObjectLambdaEvent;
import com.amazonaws.services.lambda.runtime.Context;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.WriteGetObjectResponseRequest;

import java.net.URI;
import java.net.http.HttpClient;
import java.net.http.HttpRequest;
import java.net.http.HttpResponse;
```

```
public class Example3 {

    public void handleRequest(S3ObjectLambdaEvent event, Context context) throws
 Exception {
        AmazonS3 s3Client = AmazonS3Client.builder().build();
        HttpClient httpClient = HttpClient.newBuilder().build();

        // Request the original object from S3.
        var presignedResponse = httpClient.send(
                HttpRequest.newBuilder(new URI(event.inputS3Url())).GET().build(),
                HttpResponse.BodyHandlers.ofInputStream());

        // Consume the incoming response body from the presigned request,
        // apply our transformation on that data, and emit the transformed bytes
        // into the body of the WriteGetObjectResponse request as soon as they're
 ready.
        // This example compresses the data from S3, but any processing pertinent
        // to your application can be performed here.
        var bodyStream = new GZIPCompressingInputStream(presignedResponse.body());

        // Stream the bytes back to the caller.
        s3Client.writeGetObjectResponse(new WriteGetObjectResponseRequest()
                .withRequestRoute(event.outputRoute())
                .withRequestToken(event.outputToken())
                .withInputStream(bodyStream));
    }

}
```

Python

```
import boto3
import requests
import zlib
from botocore.config import Config


"""
A helper class to work with content iterators. Takes an interator and compresses the
 bytes that come from it. It
implements 'read' and '__iter__' so that the SDK can stream the response.
"""
class Compress:
```

```
    def __init__(self, content_iter):
        self.content = content_iter
        self.compressed_obj = zlib.compressobj()

    def read(self, _size):
        for data in self.__iter__()
            return data

    def __iter__(self):
        while True:
            data = next(self.content)
            chunk = self.compressed_obj.compress(data)
            if not chunk:
                break

            yield chunk

        yield self.compressed_obj.flush()


def handler(event, context):
    """
    Setting the 'payload_signing_enabled' property to False allows us to send a
 streamed response back to the client.
    in this scenario, a streamed response means that the bytes are not buffered into
 memory as we're compressing them,
    but instead are sent straight to the user.
    """
    my_config = Config(
        region_name='eu-west-1',
        signature_version='s3v4',
        s3={
            "payload_signing_enabled": False
        }
    )
    s3 = boto3.client('s3', config=my_config)

    """
    Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    The 'userRequest' object has information related to the user who made this
 'GetObject' request to S3 Object Lambda.
```

```
    """
    get_context = event["getObjectContext"]
    route = get_context["outputRoute"]
    token = get_context["outputToken"]
    s3_url = get_context["inputS3Url"]

    # Compress the 'get' request stream.
    with requests.get(s3_url, stream=True) as r:
        compressed = Compress(r.iter_content())

        # Send the stream back to the client.
        s3.write_get_object_response(Body=compressed, RequestRoute=route,
 RequestToken=token, ContentType="text/plain",
                                     ContentEncoding="gzip")

    # Gracefully exit the Lambda function.
    return {'status_code': 200}
```

Node.js

```
const { S3 } = require('aws-sdk');
const axios = require('axios').default;
const zlib = require('zlib');

exports.handler = async (event) => {
    const s3 = new S3();

    // Retrieve the operation context object from the event. This object indicates
 where the WriteGetObjectResponse request
    // should be delivered and has a presigned URL in 'inputS3Url' where we can
 download the requested object from.
    const { getObjectContext } = event;
    const { outputRoute, outputToken, inputS3Url } = getObjectContext;

    // Download the object from S3 and process it as a stream, because it might be a
 huge object and we don't want to
    // buffer it in memory. Note the use of 'await' because we want to wait for
 'writeGetObjectResponse' to finish
    // before we can exit the Lambda function.
    await axios({
        method: 'GET',
        url: inputS3Url,
        responseType: 'stream',
```

```
    }).then(
        // Gzip the stream.
        response => response.data.pipe(zlib.createGzip())
    ).then(
        // Finally send the gzip-ed stream back to the client.
        stream => s3.writeGetObjectResponse({
            RequestRoute: outputRoute,
            RequestToken: outputToken,
            Body: stream,
            ContentType: "text/plain",
            ContentEncoding: "gzip",
        }).promise()
    );

    // Gracefully exit the Lambda function.
    return { statusCode: 200 };
}
```

> **Note**
>
> Bien que S3 Object Lambda laisse jusqu'à 60 secondes pour envoyer une réponse complète à l'appelant via la demande `WriteGetObjectResponse`, le temps réel disponible peut être inférieur. Par exemple, le délai d'expiration de votre fonction Lambda peut être inférieur à 60 secondes. Dans d'autres cas, l'appelant peut avoir des délais d'attente plus stricts.

Pour que l'appelant d'origine reçoive une réponse autre que le code de statut HTTP 500 (Erreur de serveur interne), l'appel `WriteGetObjectResponse` doit être terminé. Si la fonction Lambda renvoie une réponse, avec une exception ou autrement, avant que l'opération d'API `WriteGetObjectResponse` soit appelée, l'appelant d'origine reçoit une réponse 500 (Erreur de serveur interne). Les exceptions lancées pendant le temps nécessaire pour compléter la réponse entraînent des réponses tronquées à l'appelant. Si la fonction Lambda reçoit une réponse avec code de statut HTTP 200 (OK) de l'appel d'API `WriteGetObjectResponse`, l'appelant d'origine a envoyé la demande complète. La réponse de la fonction Lambda, qu'une exception soit déclenchée ou non, est ignorée par S3 Object Lambda.

Au moment d'appeler l'opération d'API `WriteGetObjectResponse`, Amazon S3 exige la route et le jeton de demande du contexte d'événement. Pour plus d'informations, consultez Format et utilisation du contexte d'événement.

Les paramètres de route et de jeton de demande sont nécessaires pour connecter la réponse `WriteGetObjectResult` à l'appelant d'origine. Bien qu'il soit toujours approprié de réessayer les réponses 500 (Erreur de serveur interne), car le jeton de demande est un jeton à usage unique, les tentatives ultérieures de l'utiliser peuvent entraîner des réponses avec code de statut HTTP 400 (Demande incorrecte). Bien que l'appel à `WriteGetObjectResponse` avec la route et les jetons de demande n'ait pas besoin d'être réalisé à partir de la fonction Lambda invoquée, il doit être réalisé par une identité figurant dans le même compte. L'appel doit également être terminé avant que la fonction Lambda ne termine l'exécution.

Utilisation de requêtes **`HeadObject`** dans Lambda

Cette section suppose que votre point d'accès Object Lambda est configuré pour appeler la fonction Lambda pour `HeadObject`. Lambda recevra une charge utile JSON contenant une clé appelée `headObjectContext`. Dans le contexte, il existe une propriété unique appelée `inputS3Url`, qui est une URL pré-signée pour le point d'accès de prise en charge pour `HeadObject`.

L'URL pré-signée inclura les propriétés suivantes si elles sont spécifiées :

- `versionId` (dans les paramètres de la requête)
- `requestPayer` (dans l'en-tête `x-amz-request-payer`)
- `expectedBucketOwner` (dans l'en-tête `x-amz-expected-bucket-owner`)

Les autres propriétés ne seront pas pré-signées et ne seront donc pas incluses. Les options non signées envoyées sous forme d'en-têtes peuvent être ajoutées manuellement à la demande lors de l'appel de l'URL pré-signée qui se trouve dans les en-têtes `userRequest`. Les options de chiffrement côté serveur ne sont pas prises en charge pour `HeadObject`.

Pour les paramètres d'URI de la syntaxe de la demande, consultez `HeadObject` dans la Référence des API Amazon Simple Storage Service.

L'exemple suivant illustre une charge utile d'entrée JSON de Lambda pour `HeadObject`.

```
{
  "xAmzRequestId": "requestId",
  "**headObjectContext**": {
    "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>"
  },
  "configuration": {
```

```
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
        },
        "sessionIssuer": {
            "type": "Role",
            "principalId": "principalId",
            "arn": "arn:aws:iam::111122223333:role/Admin",
            "accountId": "111122223333",
            "userName": "Admin"
            }
        }
      },
    "protocolVersion": "1.00"
}
```

Votre fonction Lambda doit renvoyer un objet JSON contenant les en-têtes et les valeurs qui seront renvoyés pour l'appel `HeadObject`.

L'exemple suivant illustre la structure du code JSON de réponse de Lambda pour `HeadObject`.

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
    "headers": {
        "Accept-Ranges": <string>,
        "x-amz-archive-status": <string>,
        "x-amz-server-side-encryption-bucket-key-enabled": <boolean>,
        "Cache-Control": <string>,
        "Content-Disposition": <string>,
        "Content-Encoding": <string>,
        "Content-Language": <string>,
        "Content-Length": <number>, // Required
        "Content-Type": <string>,
        "x-amz-delete-marker": <boolean>,
        "ETag": <string>,
        "Expires": <string>,
        "x-amz-expiration": <string>,
        "Last-Modified": <string>,
        "x-amz-missing-meta": <number>,
        "x-amz-object-lock-mode": <string>,
        "x-amz-object-lock-legal-hold": <string>,
        "x-amz-object-lock-retain-until-date": <string>,
        "x-amz-mp-parts-count": <number>,
        "x-amz-replication-status": <string>,
        "x-amz-request-charged": <string>,
        "x-amz-restore": <string>,
        "x-amz-server-side-encryption": <string>,
        "x-amz-server-side-encryption-customer-algorithm": <string>,
        "x-amz-server-side-encryption-aws-kms-key-id": <string>,
        "x-amz-server-side-encryption-customer-key-MD5": <string>,
        "x-amz-storage-class": <string>,
        "x-amz-tagging-count": <number>,
        "x-amz-version-id": <string>,
        <x-amz-meta-headers>: <string>, // user-defined metadata
        "x-amz-meta-meta1": <string>, // example of the user-defined metadata header,
 it will need the x-amz-meta prefix
        "x-amz-meta-meta2": <string>
        ...
    };
}
```

L'exemple suivant montre comment utiliser l'URL pré-signée pour renseigner votre réponse en modifiant les valeurs d'en-tête selon les besoins avant de renvoyer le code JSON.

Python

```
import requests

def lambda_handler(event, context):
    print(event)

    # Extract the presigned URL from the input.
    s3_url = event["headObjectContext"]["inputS3Url"]

    # Get the head of the object from S3.
    response = requests.head(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        return {
            "statusCode": response.status_code,
            "errorCode": "RequestFailure",
            "errorMessage": "Request to S3 failed"
    }

    # Store the headers in a dictionary.
    response_headers = dict(response.headers)

    # This obscures Content-Type in a transformation, it is optional to add
    response_headers["Content-Type"] = ""

    # Return the headers to S3 Object Lambda.
    return {
        "statusCode": response.status_code,
        "headers": response_headers
        }
```

Utilisation de requêtes **`ListObjects`** dans Lambda

Cette section suppose que votre point d'accès Object Lambda est configuré pour appeler la fonction Lambda pour `ListObjects`. Lambda recevra la charge utile JSON avec un nouvel objet nommé

`listObjectsContext`. `listObjectsContext` contient une propriété unique, `inputS3Url`, qui est une URL pré-signée pour le point d'accès de prise en charge pour `ListObjects`.

Contrairement à `GetObject` et `HeadObject`, l'URL pré-signée inclura les propriétés suivantes si elles sont spécifiées :

- Tous les paramètres de la requête
- `requestPayer` (dans l'en-tête `x-amz-request-payer`)
- `expectedBucketOwner` (dans l'en-tête `x-amz-expected-bucket-owner`)

Pour les paramètres d'URI de la syntaxe de la demande, consultez `ListObjects` dans la Référence des API Amazon Simple Storage Service.

> **Important**
>
> Nous vous recommandons d'utiliser la version la plus récente, ListObjectsV2, lorsque vous développez des applications. Pour assurer la compatibilité descendante, Amazon S3 continue de prendre en charge `ListObjects`.

L'exemple suivant illustre la charge utile d'entrée JSON de Lambda pour `ListObjects`.

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsContext**": {
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
```

```
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

Votre fonction Lambda devrait renvoyer un objet JSON contenant le code de statut, le résultat XML de liste ou les informations d'erreur qui seront renvoyées de S3 Object Lambda.

S3 Object Lambda ne traite ni ne valide `listResultXml`, mais les transmet à l'appelant `ListObjects`. Pour `listBucketResult`, S3 Object Lambda s'attend à ce que certaines propriétés soient d'un type spécifique et lèvera des exceptions s'il ne peut pas les analyser. `listResultXml` et `listBucketResult` ne peuvent pas être fournies en même temps.

L'exemple suivant montre comment utiliser l'URL pré-signée pour appeler Amazon S3 et comment utiliser le résultat pour renseigner une réponse ainsi que vérifier les erreurs.

Python

```
import requests
```

```
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsContext"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)

    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
```

```
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

L'exemple suivant illustre la structure du code JSON de réponse de Lambda pour `ListObjects`.

```
{
  "statusCode": <number>; // Required
  "errorCode": <string>;
  "errorMessage": <string>;
  "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

  "listBucketResult": {  // listBucketResult can be provided instead of listResultXml,
 however they can not both be provided in the JSON response
        "name": <string>,  // Required for 'listBucketResult'
        "prefix": <string>,
        "marker": <string>,
        "nextMarker": <string>,
        "maxKeys": <int>,   // Required for 'listBucketResult'
        "delimiter": <string>,
        "encodingType": <string>
        "isTruncated": <boolean>,  // Required for 'listBucketResult'
        "contents": [  {
            "key": <string>,  // Required for 'content'
            "lastModified": <string>,
```

```
            "eTag": <string>,
            "checksumAlgorithm": <string>,   // CRC32,  CRC32C,  SHA1,  SHA256
            "size": <int>,   // Required for 'content'
            "owner": {
                "displayName": <string>,  // Required for 'owner'
                "id": <string>,  // Required for 'owner'
            },
            "storageClass": <string>
            },
        ...
        ],
        "commonPrefixes": [  {
            "prefix": <string>   // Required for 'commonPrefix'
        },
        ...
        ],
    }
}
```

Utilisation de requêtes **`ListObjectsV2`** dans Lambda

Cette section suppose que votre point d'accès Object Lambda est configuré pour appeler la fonction Lambda pour `ListObjectsV2`. Lambda recevra la charge utile JSON avec un nouvel objet nommé `listObjectsV2Context`. `listObjectsV2Context` contient une propriété unique, `inputS3Url`, qui est une URL pré-signée pour le point d'accès de prise en charge pour `ListObjectsV2`.

Contrairement à `GetObject` et `HeadObject`, l'URL pré-signée inclura les propriétés suivantes, si elles sont spécifiées :

- Tous les paramètres de la requête
- `requestPayer` (dans l'en-tête `x-amz-request-payer`)
- `expectedBucketOwner` (dans l'en-tête `x-amz-expected-bucket-owner`)

Pour les paramètres d'URI de la syntaxe de la demande, consultez `ListObjectsV2` dans la Référence des API Amazon Simple Storage Service.

L'exemple suivant illustre la charge utile d'entrée JSON de Lambda pour `ListObjectsV2`.

```
{
    "xAmzRequestId": "requestId",
     "**listObjectsV2Context**": {
```

```
     "**inputS3Url**": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/?list-type=2&X-Amz-Security-Token=<snip>",
     },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
        }
    },
  "protocolVersion": "1.00"
}
```

Votre fonction Lambda devrait renvoyer un objet JSON contenant le code de statut, le résultat XML de liste ou les informations d'erreur qui seront renvoyées de S3 Object Lambda.

S3 Object Lambda ne traite ni ne valide `listResultXml`, mais les transmet à l'appelant `ListObjectsV2`. Pour `listBucketResult`, S3 Object Lambda s'attend à ce que certaines propriétés soient d'un type spécifique et lèvera des exceptions s'il ne peut pas les analyser. `listResultXml` et `listBucketResult` ne peuvent pas être fournies en même temps.

L'exemple suivant montre comment utiliser l'URL pré-signée pour appeler Amazon S3 et comment utiliser le résultat pour renseigner une réponse ainsi que vérifier les erreurs.

Python

```
import requests
import xmltodict

def lambda_handler(event, context):
    # Extract the presigned URL from the input.
    s3_url = event["listObjectsV2Context"]["inputS3Url"]


    # Get the head of the object from Amazon S3.
    response = requests.get(s3_url)

    # Return the error to S3 Object Lambda (if applicable).
    if (response.status_code >= 400):
        error = xmltodict.parse(response.content)
        return {
            "statusCode": response.status_code,
            "errorCode": error["Error"]["Code"],
            "errorMessage": error["Error"]["Message"]
        }

    # Store the XML result in a dict.
    response_dict = xmltodict.parse(response.content)

    # This obscures StorageClass in a transformation, it is optional to add
    for item in response_dict['ListBucketResult']['Contents']:
        item['StorageClass'] = ""

    # Convert back to XML.
    listResultXml = xmltodict.unparse(response_dict)
```

```
    # Create response with listResultXml.
    response_with_list_result_xml = {
        'statusCode': 200,
        'listResultXml': listResultXml
    }

    # Create response with listBucketResult.
    response_dict['ListBucketResult'] =
 sanitize_response_dict(response_dict['ListBucketResult'])
    response_with_list_bucket_result = {
        'statusCode': 200,
        'listBucketResult': response_dict['ListBucketResult']
    }

    # Return the list to S3 Object Lambda.
    # Can return response_with_list_result_xml or response_with_list_bucket_result
    return response_with_list_result_xml

# Converting the response_dict's key to correct casing
def sanitize_response_dict(response_dict: dict):
    new_response_dict = dict()
    for key, value in response_dict.items():
        new_key = key[0].lower() + key[1:] if key != "ID" else 'id'
        if type(value) == list:
            newlist = []
            for element in value:
                if type(element) == type(dict()):
                    element = sanitize_response_dict(element)
                newlist.append(element)
            value = newlist
        elif type(value) == dict:
            value = sanitize_response_dict(value)
        new_response_dict[new_key] = value
    return new_response_dict
```

L'exemple suivant illustre la structure du code JSON de réponse de Lambda pour `ListObjectsV2`.

```
{
    "statusCode": <number>; // Required
    "errorCode": <string>;
    "errorMessage": <string>;
```

```
    "listResultXml": <string>; // This can also be Error XML string in case S3 returned
 error response when calling the pre-signed URL

    "listBucketResult": {  // listBucketResult can be provided instead of
 listResultXml, however they can not both be provided in the JSON response
        "name": <string>, // Required for 'listBucketResult'
        "prefix": <string>,
        "startAfter": <string>,
        "continuationToken": <string>,
        "nextContinuationToken": <string>,
        "keyCount": <int>, // Required for 'listBucketResult'
        "maxKeys": <int>, // Required for 'listBucketResult'
        "delimiter": <string>,
        "encodingType": <string>
        "isTruncated": <boolean>, // Required for 'listBucketResult'
        "contents": [ {
            "key": <string>, // Required for 'content'
            "lastModified": <string>,
            "eTag": <string>,
            "checksumAlgorithm": <string>, // CRC32, CRC32C, SHA1, SHA256
            "size": <int>, // Required for 'content'
            "owner": {
                "displayName": <string>, // Required for 'owner'
                "id": <string>, // Required for 'owner'
            },
            "storageClass": <string>
            },
            ...
        ],
        "commonPrefixes": [ {
            "prefix": <string> // Required for 'commonPrefix'
            },
        ...
        ],
    }
}
```

Format et utilisation du contexte d'événement

Amazon S3 Object Lambda fournit le contexte de la demande effectuée lors de l'événement transmis à votre AWS Lambda fonction. Voici un exemple de demande. Les descriptions des champs sont incluses après l'exemple.

```
{
    "xAmzRequestId": "requestId",
    "getObjectContext": {
        "inputS3Url": "https://my-s3-ap-111122223333.s3-accesspoint.us-
east-1.amazonaws.com/example?X-Amz-Security-Token=<snip>",
        "outputRoute": "io-use1-001",
        "outputToken": "OutputToken"
    },
    "configuration": {
        "accessPointArn": "arn:aws:s3-object-lambda:us-
east-1:111122223333:accesspoint/example-object-lambda-ap",
        "supportingAccessPointArn": "arn:aws:s3:us-
east-1:111122223333:accesspoint/example-ap",
        "payload": "{}"
    },
    "userRequest": {
        "url": "https://object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com/example",
        "headers": {
            "Host": "object-lambda-111122223333.s3-object-lambda.us-
east-1.amazonaws.com",
            "Accept-Encoding": "identity",
            "X-Amz-Content-SHA256": "e3b0c44298fc1example"
        }
    },
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "principalId",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/example",
        "accountId": "111122223333",
        "accessKeyId": "accessKeyId",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "Wed Mar 10 23:41:52 UTC 2021"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "principalId",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            }
```

```
        }
    },
    "protocolVersion": "1.00"
}
```

Les champs suivants sont inclus dans la demande :

- `xAmzRequestId` – ID de demande Amazon S3 pour cette demande. Nous vous recommandons de consigner cette valeur pour faciliter le débogage.
- `getObjectContext` – Détails d'entrée et de sortie pour les connexions à Amazon S3 et S3 Object Lambda.
  - `inputS3Url` – URL pré-signée qui peut être utilisée pour récupérer l'objet d'origine depuis Amazon S3. L'URL est signée avec l'identité de l'appelant d'origine et les autorisations de cet utilisateur s'appliquent quand l'URL est utilisée. S'il y a des en-têtes signés dans cette URL, la fonction Lambda doit les inclure dans l'appel à Amazon S3, à l'exception de l'en-tête `Host`.
  - `outputRoute` – Un jeton de routage qui est ajouté à l'URL S3 Object Lambda lorsque la fonction Lambda appelle `WriteGetObjectResponse`.
  - `outputToken` – Jeton opaque utilisé par S3 Object Lambda pour mettre en correspondance l'appel `WriteGetObjectResponse` avec l'appelant d'origine.
- `configuration` : informations de configuration sur le point d'accès Object Lambda.
  - `accessPointArn` : Amazon Resource Name (ARN) du point d'accès Object Lambda qui a reçu cette demande.
  - `supportingAccessPointArn` : ARN du point d'accès de prise en charge spécifié dans la configuration du point d'accès Object Lambda.
  - `payload` : données personnalisées qui sont appliquées à la configuration du point d'accès Object Lambda. S3 Object Lambda considère ces données comme une chaîne opaque. Dès lors, elles devront peut-être être décodées avant utilisation.
- `userRequest` – Informations sur l'appel d'origine à S3 Object Lambda.
  - `url` – URL décodée de la demande telle qu'elle a été reçue par S3 Object Lambda, à l'exclusion des paramètres de requête liés à l'autorisation.
  - `headers` – Carte de chaîne aux chaînes contenant les en-têtes HTTP et leurs valeurs de l'appel d'origine, à l'exclusion de tous les en-têtes liés à l'autorisation. Si le même en-tête apparaît plusieurs fois, les valeurs de chaque instance du même en-tête sont combinées dans une liste délimitée par des virgules. Le cas des en-têtes d'origine est conservé dans cette carte.

- `userIdentity` – Détails sur l'identité qui a adressé l'appel à S3 Object Lambda. Pour plus d'informations, consultez Consignation d'événements de données pour les journaux d'activité dans le Guide de l'utilisateur AWS CloudTrail .
  - `type` – Type d'identité.
  - `accountId`— Compte AWS À laquelle appartient l'identité.
  - `userName` – Nom descriptif de l'identité qui a réalisé l'appel.
  - `principalId` – Identifiant unique de l'entité qui a effectué l'appel.
  - `arn` – ARN du principal qui a effectué l'appel. La dernière partie de l'ARN contient l'utilisateur ou le rôle qui a réalisé l'appel.
  - `sessionContext` – Si la demande a été effectuée avec les autorisations de sécurité temporaires, cet élément fournit des informations sur la session qui a été créée pour ces autorisations.
  - `invokedBy`— Le nom de la personne à Service AWS l'origine de la demande, par exemple Amazon EC2 Auto Scaling ou AWS Elastic Beanstalk.
  - `sessionIssuer` – Si la demande a été effectuée avec des informations d'identification de sécurité temporaires, cet élément fournit des informations sur la façon dont les autorisations ont été obtenues.
- `protocolVersion` – ID de version du contexte fourni. Le format de ce champ est `{Major Version}.{Minor Version}`. Les numéros de version mineure sont toujours des nombres à deux chiffres. Toute suppression ou modification de la sémantique d'un champ nécessite un changement de version majeur et une participation active. Simple Storage Service (Amazon S3) peut ajouter de nouveaux champs à tout moment, auquel cas vous risquez de rencontrer un changement de version mineure. En raison de la nature des déploiements logiciels, il est possible que plusieurs versions mineures soient utilisées simultanément.

Utilisation des en-têtes Range et partNumber

Lorsque vous travaillez avec des objets volumineux dans Amazon S3 Object Lambda, vous pouvez utiliser l'en-tête HTTP `Range` pour télécharger une plage d'octets spécifiée à partir d'un objet. Pour extraire différentes plages d'octets à partir d'un même objet, utilisez des connexions simultanées à Amazon S3. Spécifiez également le paramètre `partNumber` (entier compris entre 1 et 10 000) pour exécuter une demande « par plage » pour la partie spécifiée de l'objet.

Étant donné qu'il existe plusieurs façons de gérer une demande qui inclut le paramètre `Range` ou `partNumber`, S3 Object Lambda n'applique pas ces paramètres à l'objet transformé. Votre AWS Lambda fonction doit plutôt implémenter cette fonctionnalité selon les besoins de votre application.

Pour utiliser les paramètres `Range` et `partNumber` avec S3 Object Lambda, procédez comme suit :

- Activez ces paramètres dans la configuration de vos points d'accès Object Lambda.
- Écrivez une fonction Lambda capable de gérer les demandes qui incluent ces paramètres.

Les étapes suivantes expliquent comment procéder.

Étape 1 : configurer votre point d'accès Object Lambda

Par défaut, les points d'accès Object Lambda répondent avec une erreur de code de statut HTTP 501 (Non implémenté) à toute requête `GetObject` ou `HeadObject` contenant un paramètre `Range` ou `partNumber`, que ce soit dans les en-têtes ou les paramètres de requête.

Pour permettre à un point d'accès Object Lambda d'accepter ces demandes, vous devez inclure `GetObject-Range`, `GetObject-PartNumber`, `HeadObject-Range` ou `HeadObject-PartNumber` dans la section `AllowedFeatures` de la configuration de votre point d'accès Object Lambda. Pour plus d'informations sur la mise à jour de votre configuration de point d'accès Object Lambda, consultez Création de points d'accès Object Lambda.

Étape 2 : implémenter la gestion de **`Range`** ou **`partNumber`** dans votre fonction Lambda

Lorsque votre point d'accès Object Lambda invoque votre fonction Lambda avec une demande `GetObject` ou `HeadObject` par plage, le paramètre `Range` ou `partNumber` est inclus dans le contexte de l'événement. L'emplacement du paramètre dans le contexte d'événement dépend du paramètre utilisé et de la façon dont il a été inclus dans la demande d'origine au point d'accès Object Lambda, comme expliqué dans le tableau suivant.

Paramètre	Emplacement du contexte d'événement
`Range` (en-tête)	`userRequest.headers.Range`
`Range` (paramètre de la demande)	`userRequest.url` (paramètre `Range` de la demande)
`partNumber`	`userRequest.url` (paramètre `partNumber` de la demande)

> **Important**
>
> L'URL pré-signée fournie pour votre point d'accès Object Lambda ne contient pas le paramètre `Range` ou `partNumber` de la demande d'origine. Consultez les options suivantes pour savoir comment gérer ces paramètres dans votre AWS Lambda fonction.

Après avoir extrait la valeur `Range` ou `partNumber`, vous pouvez adopter l'une des approches suivantes en fonction des besoins de votre application :

A. Mapper le paramètre **`Range`** ou **`partNumber`** demandé à l'objet transformé (recommandé)

La méthode la plus fiable pour traiter les requêtes `Range` et `partNumber` consiste à effectuer les opérations suivantes :

- Récupérez l'objet complet à partir d'Amazon S3.
- Transformez l'objet.
- Appliquez le paramètre `Range` ou `partNumber` demandé à l'objet transformé.

Pour ce faire, utilisez l'URL pré-signée fournie afin de récupérer l'objet entier d'Amazon S3, puis traitez l'objet au besoin. Pour un exemple de fonction Lambda qui traite un `Range` paramètre de cette manière, consultez cet exemple dans le référentiel AWS Samples GitHub .

B. Mappez l'élément **`Range`** demandé sur l'URL pré-signée.

Dans certains cas, votre fonction Lambda peut mapper l'élément `Range` demandé directement sur l'URL pré-signée pour récupérer uniquement une partie de l'objet à partir d'Amazon S3. Cette approche n'est appropriée que si votre transformation répond aux deux critères suivants :

1. Votre fonction de transformation peut être appliquée à des plages d'objets partielles.
2. L'application du paramètre `Range` avant ou après la fonction de transformation aboutit au même objet transformé.

Par exemple, une fonction de transformation qui convertit tous les caractères d'un objet codé en ASCII en majuscules répond aux deux critères précédents. La transformation peut être appliquée à une partie d'un objet, et l'application du paramètre `Range` avant la transformation donne le même résultat que son application après la transformation.

En revanche, une fonction qui rétablit les caractères d'un objet codé en ASCII ne répond pas à ces critères. Cette fonction répond au critère 1, car elle peut être appliquée à des plages d'objets

partielles. Cependant, elle ne répond pas au critère 2, car le paramètre `Range` appliqué avant la transformation ne donne pas le même résultat que lorsqu'il est appliqué après la transformation.

Prenons une demande d'application de la fonction aux trois premiers caractères d'un objet avec le contenu `abcdefg`. Si le paramètre `Range` est appliqué avant la transformation, il récupère uniquement `abc`, puis rétablit les données et renvoie `cba`. Mais si le paramètre est appliqué après la transformation, la fonction récupère l'objet entier, le rétablit, puis applique le paramètre `Range` et renvoie `gfe`. Étant donné que ces résultats sont différents, cette fonction ne doit pas appliquer le paramètre `Range` lors de la récupération de l'objet à partir d'Amazon S3. À la place, elle doit récupérer l'objet entier, effectuer la transformation, et seulement alors appliquer le paramètre `Range`.

> **Warning**
>
> Dans de nombreux cas, l'application du paramètre `Range` à l'URL pré-signée entraîne un comportement inattendu de la fonction Lambda ou du client demandeur. À moins que vous ne soyez sûr que votre application fonctionne correctement lorsque vous récupérez uniquement un objet partiel d'Amazon S3, nous vous recommandons de récupérer et de transformer des objets complets comme décrit précédemment dans l'approche A.

Si votre application répond aux critères décrits précédemment dans l'approche B, vous pouvez simplifier votre AWS Lambda fonction en récupérant uniquement la plage d'objets demandée, puis en exécutant votre transformation sur cette plage.

L'exemple de code Java suivant montre comment effectuer les opérations suivantes :

- Récupérer l'en-tête `Range` de la requête `GetObject`.
- Ajouter l'en-tête `Range` à l'URL pré-signée que Lambda peut utiliser pour récupérer la plage demandée à partir d'Amazon S3.

```
private HttpRequest.Builder applyRangeHeader(ObjectLambdaEvent event,
 HttpRequest.Builder presignedRequest) {
    var header = event.getUserRequest().getHeaders().entrySet().stream()
            .filter(e -> e.getKey().toLowerCase(Locale.ROOT).equals("range"))
            .findFirst();

    // Add check in the query string itself.
```

```
    header.ifPresent(entry -> presignedRequest.header(entry.getKey(),
 entry.getValue()));
    return presignedRequest;
}
```

Utilisation de AWS fonctions Lambda intégrées

AWS fournit des AWS Lambda fonctions prédéfinies que vous pouvez utiliser avec Amazon S3 Object Lambda pour détecter et supprimer les informations personnelles identifiables (PII) et décompresser les objets S3. Ces fonctions Lambda sont disponibles dans AWS Serverless Application Repository. Vous pouvez sélectionner ces fonctions via la AWS Management Console lorsque vous créez votre point d'accès Object Lambda.

Pour plus d'informations sur le déploiement d'applications sans serveur depuis le AWS Serverless Application Repository, consultez la section Déploiement d'applications dans le guide du AWS Serverless Application Repository développeur.

> **Note**
>
> Les exemples suivants peuvent être utilisés uniquement avec des requêtes `GetObject`.

Exemple 1 : contrôle d'accès aux données d'identification personnelle (PII)

Cette fonction Lambda utilise Amazon Comprehend, un service de traitement du langage naturel (NLP) qui a recours au machine learning pour identifier des informations et des relations dans un texte. Elle détecte automatiquement les données d'identification personnelle (PII), telles que les noms, adresses, dates, numéros de carte de crédit et numéros de sécurité sociale, dans les documents figurant dans votre compartiment Amazon S3. Si vous avez des documents dans votre compartiment qui incluent des données PII, vous pouvez configurer la fonction PII Access Control pour détecter ces types d'entités PII et en bloquer l'accès aux utilisateurs non autorisés.

Pour commencer, déployez la fonction Lambda suivante dans votre compte et ajoutez l'Amazon Resource Name (ARN) de cette fonction dans la configuration de votre point d'accès Object Lambda.

Voici un exemple d'ARN pour cette fonction :

```
arn:aws:serverlessrepo:us-east-1:111122223333:applications/
ComprehendPiiAccessControlS3ObjectLambda
```

Vous pouvez ajouter ou consulter cette fonction sur AWS Management Console le AWS Serverless Application Repository lien suivant : ComprehendPiiAccessControlS3 ObjectLambda.

Pour afficher cette fonction GitHub, consultez Amazon Comprehend S3 Object Lambda.

Exemple 2 : rédaction de données d'identification personnelle (PII)

Cette fonction Lambda utilise Amazon Comprehend, un service de traitement du langage naturel (NLP) qui a recours au machine learning pour identifier des informations et des relations dans un texte. Elle supprime automatiquement les données d'identification personnelle (PII), telles que les noms, adresses, dates, numéros de carte de crédit et numéros de sécurité sociale, dans les documents figurant dans votre compartiment Amazon S3.

Si vous avez des documents dans votre compartiment qui incluent des informations telles que des numéros de carte de crédit ou des informations de compte bancaire, vous pouvez configurer la fonction S3 Object Lambda Rédaction de PII pour détecter les PII, puis renvoyer une copie de ces documents dans lesquels les types d'entités PII sont expurgés.

Pour commencer, déployez la fonction Lambda suivante dans votre compte et ajoutez l'ARN de cette fonction dans la configuration de votre point d'accès Object Lambda.

Voici un exemple d'ARN pour cette fonction :

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/
ComprehendPiiRedactionS3ObjectLambda
```

Vous pouvez ajouter ou consulter cette fonction sur AWS Management Console le AWS Serverless Application Repository lien suivant : ComprehendPiiRedactionS3 ObjectLambda.

Pour afficher cette fonction GitHub, consultez Amazon Comprehend S3 Object Lambda.

Pour en savoir plus sur end-to-end les procédures complètes relatives à certaines tâches Lambda d'objets S3 dans la rédaction d'informations personnelles, consultez. Didacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend

Exemple 3 : Décompression

La fonction Lambda `S3ObjectLambdaDecompression` peut décompresser les objets stockés dans Amazon S3 dans l'un des six formats de fichiers compressés suivants : `bzip2`, `gzip`, `snappy`, `zlib`, `zstandard` ou `ZIP`.

Pour commencer, déployez la fonction Lambda suivante dans votre compte et ajoutez l'ARN de cette fonction dans la configuration de votre point d'accès Object Lambda.

Voici un exemple d'ARN pour cette fonction :

```
arn:aws:serverlessrepo:us-east-1:111122223333::applications/S3ObjectLambdaDecompression
```

Vous pouvez ajouter ou consulter cette fonction sur AWS Management Console le AWS Serverless Application Repository lien suivant : S3 ObjectLambdaDecompression.

Pour afficher cette fonction GitHub, consultez la section Décompression Lambda d'objets S3.

Bonnes pratiques et directives pour S3 Object Lambda

Lorsque vous utilisez S3 Object Lambda, suivez ces bonnes pratiques et directives pour optimiser les opérations et les performances.

Rubriques

- Utilisation de S3 Object Lambda
- Services AWS utilisé en relation avec S3 Object Lambda
- En-têtes Range et partNumber
- Transformation de la date expiry-date
- Travailler avec le AWS CLI et AWS SDKs

Utilisation de S3 Object Lambda

S3 Object Lambda prend en charge uniquement le traitement des requêtes `GET`, `LIST` et `HEAD`. Aucune autre demande n'invoque mais renvoie AWS Lambda des réponses d'API standard non transformées. Vous pouvez créer un maximum de 1 000 points d'accès Object Lambda Compte AWS par région. La AWS Lambda fonction que vous utilisez doit se trouver dans la même Compte AWS région que le point d'accès Object Lambda.

S3 Object Lambda accorde jusqu'à 60 secondes pour diffuser une réponse complète à son mandataire. Votre fonction est également soumise à des quotas AWS Lambda par défaut. Pour plus d'informations, consultez Quotas Lambda dans le Guide du développeur AWS Lambda .

Quand S3 Object Lambda invoque votre fonction Lambda spécifiée, il vous incombe de veiller à ce que toutes les données écrasées ou supprimées d'Amazon S3 par votre fonction ou application Lambda spécifiée sont volontaires et correctes.

Vous pouvez utiliser S3 Object Lambda uniquement pour effectuer des opérations sur des objets. Vous ne pouvez pas utiliser S3 Object Lambda pour effectuer d'autres opérations Amazon S3, comme modifier ou supprimer des compartiments. Pour obtenir la liste complète des opérations S3 qui prennent en charge les points d'accès, consultez Compatibilité des points d'accès avec les opérations S3.

Outre cette liste, les points d'accès Object Lambda ne prennent pas en charge les opérations d'API `POST Object`, `CopyObject` (en tant que source) ou `SelectObjectContent`.

Services AWS utilisé en relation avec S3 Object Lambda

S3 Object Lambda connecte Amazon S3 et, éventuellement AWS Lambda, les autres appareils Services AWS de votre choix pour fournir des objets adaptés aux applications demandeuses. Toutes les Services AWS applications utilisées avec S3 Object Lambda sont régies par leurs accords de niveau de service respectifs ()SLAs. Par exemple, si l'un d'entre eux Service AWS ne respecte pas son engagement de service, vous pouvez bénéficier d'un crédit de service, comme indiqué dans le SLA du service.

En-têtes **`Range`** et **`partNumber`**

Lorsque vous utilisez des objets volumineux, vous pouvez avoir recours à l'en-tête HTTP `Range` pour télécharger une plage d'octets donnée à partir d'un objet. Lorsque vous utilisez l'en-tête `Range`, votre demande extrait uniquement la partie spécifiée de l'objet. Vous pouvez également utiliser l'en-tête `partNumber` pour effectuer une requête par plage pour la partie spécifiée de l'objet.

Pour de plus amples informations, veuillez consulter Utilisation des en-têtes Range et partNumber.

Transformation de la date **`expiry-date`**

Vous pouvez ouvrir ou télécharger des objets transformés depuis votre point d'accès Object Lambda sur le. AWS Management Console Ces objets ne doivent pas avoir expiré. Si votre fonction Lambda transforme la date `expiry-date` de vos objets, vous pouvez voir des objets expirés qui ne peuvent pas être ouverts ou téléchargés. Ce comportement s'applique uniquement aux objets restaurés S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.

Travailler avec le AWS CLI et AWS SDKs

AWS Command Line Interface (AWS CLI) Les sous-commandes S3 (`cp`,`mv`, et`sync`) et l'utilisation de la AWS SDK pour Java `TransferManager` classe ne sont pas prises en charge pour une utilisation avec S3 Object Lambda.

Didacticiels S3 Object Lambda

Les didacticiels suivants présentent end-to-end des procédures complètes pour certaines tâches S3 Object Lambda.

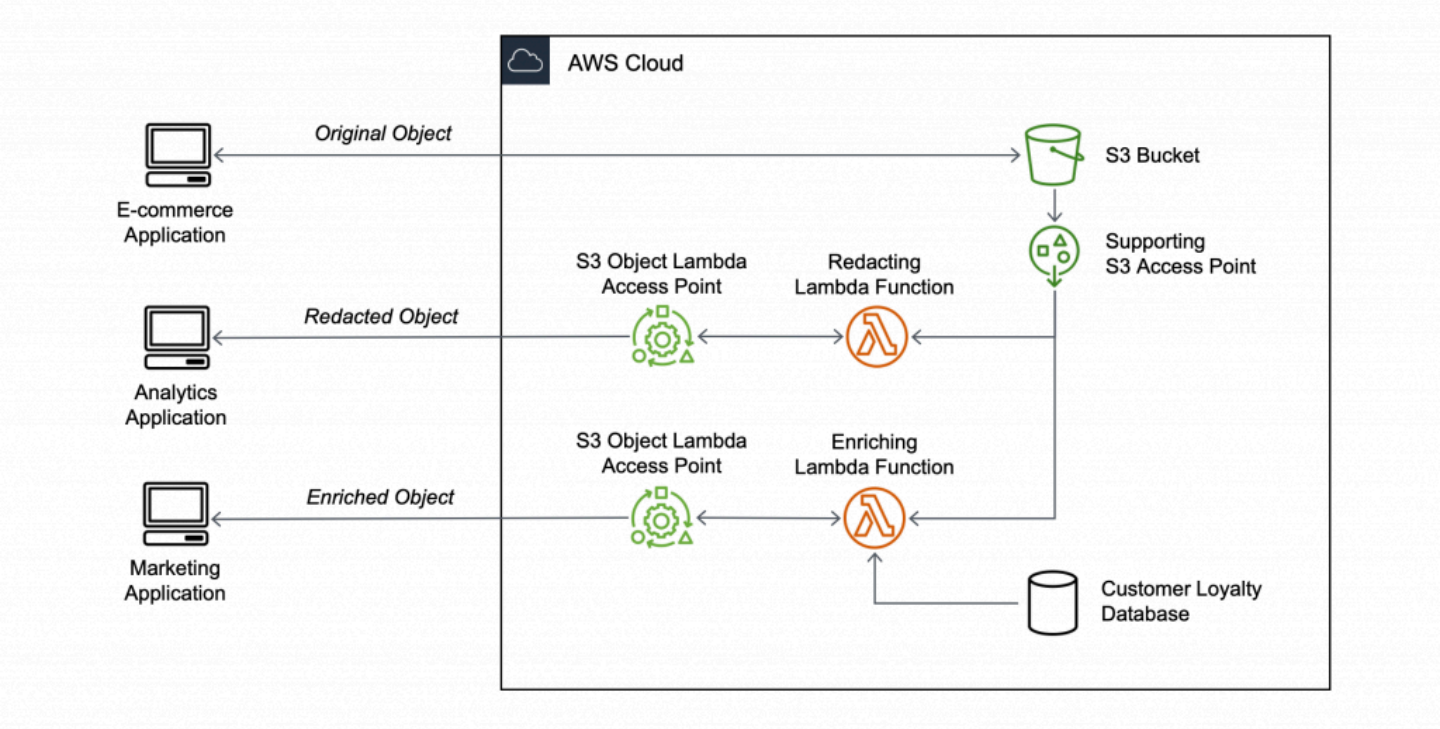
Avec S3 Object Lambda, vous pouvez ajouter votre propre code pour traiter les données récupérées à partir de S3 avant de les renvoyer vers une application. Chacun des didacticiels suivants modifie les données au fur et à mesure qu'elles sont extraites d'Amazon S3, sans modifier l'objet existant ni conserver plusieurs copies des données. Le premier didacticiel expliquera comment ajouter une AWS Lambda fonction à une requête GET S3 pour modifier un objet extrait de S3. Le deuxième didacticiel montre comment utiliser une fonction Lambda prédéfinie basée sur Amazon Comprehend pour protéger les données d'identification personnelle (PII) récupérées à partir de S3 avant de les renvoyer à une application. Le troisième didacticiel utilise S3 Object Lambda pour ajouter un filigrane à une image telle qu'elle est extraite d'Amazon S3.

- Didacticiel : Transformation de données pour votre application avec S3 Object Lambda
- Didacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend
- Tutoriel : Utilisation de S3 Object Lambda pour filigraner dynamiquement des images au fur et à mesure de leur récupération

Didacticiel : Transformation de données pour votre application avec S3 Object Lambda

Lorsque vous stockez des données dans Amazon S3, vous pouvez facilement les partager pour utilisation par plusieurs applications. Cependant, chaque application peut avoir des exigences de format de données uniques et nécessiter une modification ou un traitement de vos données pour un cas d'utilisation particulier. Par exemple, un jeu de données créé par une application de commerce électronique peut inclure des données d'identification personnelle (PII). Lorsque les mêmes données sont traitées à des fins analytiques, ces DCPI ne sont pas nécessaires et doivent être supprimées. Toutefois, si le même jeu de données est utilisé pour une campagne marketing, vous devrez peut-être enrichir les données avec des détails supplémentaires, comme des informations provenant de la base de données de fidélisation des clients.

Avec S3 Object Lambda, vous pouvez ajouter votre propre code pour traiter les données récupérées à partir de S3 avant de les renvoyer vers une application. Plus précisément, vous pouvez configurer une AWS Lambda fonction et l'associer à un point d'accès Lambda S3 Object. Lorsqu'une application envoie des requêtes S3 GET standard via le point d'accès S3 Object Lambda, la fonction Lambda spécifiée est invoquée pour traiter toutes les données extraites de la source de données sous-jacente via le point d'accès S3 compatible. Ensuite, le point d'accès S3 Object Lambda renvoie le résultat transformé à l'application. Vous pouvez créer et exécuter vos propres fonctions Lambda personnalisées, en adaptant la transformation des données S3 Object Lambda à votre cas d'utilisation particulier, sans devoir modifier vos applications.



Objectif

Dans ce didacticiel, vous apprendrez à ajouter du code personnalisé aux demandes GET S3 standard pour modifier l'objet demandé récupéré à partir de S3 afin que l'objet réponde aux besoins du client ou de l'application demandeur. Plus précisément, vous apprendrez à transformer tout le texte de l'objet d'origine stocké dans un compartiment S3 en majuscules via S3 Object Lambda.

> **Note**
>
> Ce didacticiel utilise le code Python pour transformer les données. Pour des exemples, AWS SDKs voir Transformer des données pour votre application avec S3 Object Lambda dans la bibliothèque d'exemples de code du AWS SDK.

Rubriques

- Prérequis
- Étape 1 : créer un compartiment S3
- Étape 2 : charger un fichier dans le compartiment S3
- Étape 3 : créer un point d'accès S3
- Étape 4 : créer une fonction Lambda
- Étape 5 : configurer une politique IAM pour le rôle d'exécution de votre fonction Lambda
- Étape 6 : créer un point d'accès S3 Object Lambda
- Étape 7 : afficher les données transformées
- Étape 8 : nettoyer
- Étapes suivantes

Prérequis

Avant de commencer ce didacticiel, vous devez disposer d'un utilisateur Compte AWS auquel vous pouvez vous connecter en tant qu'utilisateur AWS Identity and Access Management (IAM) avec les autorisations appropriées. Vous devez également installer Python 3.8 ou version ultérieure.

Sous-étapes

- Créez un utilisateur IAM avec des autorisations dans votre Compte AWS (console)
- Installez Python 3.8 ou version ultérieure sur votre machine locale

Créez un utilisateur IAM avec des autorisations dans votre Compte AWS (console)

Vous pouvez créer un utilisateur IAM pour le didacticiel. Pour terminer ce didacticiel, votre utilisateur IAM doit joindre les politiques IAM suivantes pour accéder aux AWS ressources pertinentes et

effectuer des actions spécifiques. Pour en savoir plus sur la création d'un utilisateur IAM, consultez Créer des utilisateurs IAM (console) dans le guide de l'utilisateur IAM.

Votre utilisateur IAM requiert les politiques suivantes :

- AmazonS3 FullAccess — Accorde des autorisations pour toutes les actions Amazon S3, y compris les autorisations pour créer et utiliser un point d'accès Object Lambda.
- AWSLambda_FullAccess— Accorde des autorisations à toutes les actions Lambda.
- IAMFullAccès : accorde des autorisations à toutes les actions IAM.
- IAMAccessAnalyzerReadOnlyAccess— Accorde l'autorisation de lire toutes les informations d'accès fournies par IAM Access Analyzer.
- CloudWatchLogsFullAccess— Accorde un accès complet aux CloudWatch journaux.

> **Note**
>
> Pour des raisons de simplicité, ce didacticiel crée et utilise un utilisateur IAM. Après avoir terminé ce didacticiel, n'oubliez pas de Supprimer l'utilisateur IAM. Pour une utilisation en production, nous vous recommandons de suivre les Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM. Une bonne pratique requiert que les utilisateurs humains utilisent une fédération avec un fournisseur d'identité pour accéder à AWS avec des informations d'identification temporaires. Une autre bonne pratique consiste à exiger que les charges de travail utilisent des informations d'identification temporaires avec des rôles IAM pour accéder à AWS. Pour en savoir plus sur l'utilisation AWS IAM Identity Center pour créer des utilisateurs avec des informations d'identification temporaires, voir Getting started dans le guide de AWS IAM Identity Center l'utilisateur.
> Ce didacticiel utilise des politiques gérées par AWS à accès complet. Pour utilisation en production, nous vous recommandons d'accorder uniquement les autorisations minimales nécessaires à votre cas d'utilisation, conformément aux Bonnes pratiques de sécurité.

Installez Python 3.8 ou version ultérieure sur votre machine locale

Utilisez la procédure suivante pour installer Python 3.8 ou version ultérieure sur votre machine locale. Pour obtenir des instructions sur l'installation, consultez la page Télécharger Python dans le Guide du débutant de Python.

1. Ouvrez votre terminal ou shell local, puis exécutez la commande suivante afin de déterminer si Python est déjà installé et, si oui, quelle version est installée.

   ```
   python --version
   ```

2. Si Python 3.8 ou version ultérieure n'est pas installé, téléchargez le programme d'installation officiel de Python 3.8 ou version ultérieure qui convient à votre machine locale.
3. Exécutez le programme d'installation en double-cliquant sur le fichier téléchargé, puis suivez les étapes pour achever l'installation.

   Pour les utilisateurs Windows, choisissez Ajouter Python 3.X au PATH dans l'assistant d'installation avant de choisir Installer maintenant.
4. Redémarrez votre terminal en le fermant et en le rouvrant.
5. Exécutez la commande suivante pour vérifier que Python 3.8 ou version ultérieure est installé correctement.

   Pour les utilisateurs macOS, exécutez cette commande :

   ```
   python3 --version
   ```

   Pour les utilisateurs Windows, exécutez cette commande :

   ```
   python --version
   ```

6. Exécutez les commandes suivantes pour vérifier que le gestionnaire de paquets pip3 est installé. Si vous voyez un numéro de version pip et Python 3.8 ou version ultérieure dans la réponse de la commande, cela signifie que le gestionnaire de paquets pip3 est installé correctement.

   ```
   pip --version
   ```

Étape 1 : créer un compartiment S3

Créez un compartiment pour stocker les données originales que vous prévoyez de transformer.

> **Note**
>
> Des points d'accès peuvent être attachés à une autre source de données, telle qu'un volume Amazon FSx pour OpenZFS, mais ce didacticiel utilise un point d'accès auxiliaire attaché à un compartiment S3.

Pour créer un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Choisissez Créer un compartiment.

   La page Créer un compartiment s'ouvre.
4. Pour Nom du compartiment, saisissez un nom (par exemple, **`tutorial-bucket`**) pour votre compartiment.

   Pour en savoir plus sur les règles d'attribution de noms des compartiments Amazon S3, consultez Règles de dénomination des compartiments à usage général.
5. Pour Région, choisissez l' Région AWS endroit où vous souhaitez que le compartiment réside.

   Pour en savoir plus sur les régions des compartiments, consultez Présentation des compartiments à usage général.
6. Pour Paramètres de blocage de l'accès public à ce compartiment, conservez les paramètres par défaut (Bloquer tout accès public est activé).

   Nous vous recommandons de laisser tous les paramètres de blocage de l'accès public activés, sauf si vous devez en désactiver un ou plusieurs pour votre cas d'utilisation. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.
7. Pour les paramètres restants, conservez les paramètres par défaut.

   (Facultatif) Si vous souhaitez configurer des paramètres de compartiment supplémentaires pour votre cas d'utilisation particulier, consultez Création d'un bucket à usage général.
8. Choisissez Créer un compartiment.

Étape 2 : charger un fichier dans le compartiment S3

Chargez un fichier texte dans le compartiment S3. Ce fichier texte contient les données originales que vous transformerez en majuscules plus tard dans ce didacticiel.

Par exemple, vous pouvez charger un fichier `tutorial.txt` qui contient le texte suivant :

```
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.
```

Charger un fichier dans un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment que vous avez créé à l'étape 1 (par exemple, **`tutorial-bucket`**) pour y charger votre fichier.
4. Sous l'onglet Objets de votre compartiment, choisissez Charger.
5. Dans la page Charger, sous Fichiers et dossiers, choisissez Ajouter des fichiers.
6. Choisissez un fichier à charger, puis choisissez Ouvrir. Par exemple, vous pouvez charger le fichier `tutorial.txt` mentionné précédemment.
7. Choisissez Charger.

Étape 3 : créer un point d'accès S3

Pour utiliser un point d'accès S3 Object Lambda afin d'accéder aux données originales et de les transformer, vous devez créer un point d'accès S3 et l'associer au compartiment S3 que vous avez créé à l'étape 1. Le point d'accès doit se trouver dans le même Région AWS emplacement que les objets que vous souhaitez transformer.

Plus loin dans ce didacticiel, vous utiliserez ce point d'accès comme point d'accès de prise en charge pour votre point d'accès Object Lambda.

Créer un point d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation, choisissez Points d'accès.
3. Dans la page Points d'accès, choisissez Créer un point d'accès.
4. Dans le champ Nom du point d'accès, saisissez le nom (par exemple, **`tutorial-access-point`**) du point d'accès.

   Pour en savoir plus sur l'attribution de noms aux points d'accès, consultez Règles de dénomination pour les points d'accès.
5. Dans le champ Source de données, entrez le nom du bucket que vous avez créé à l'étape 1 (par exemple,**`tutorial-bucket`**). S3 attache le point d'accès à ce compartiment.

   (Facultatif) Vous pouvez choisir Parcourir S3 pour parcourir et rechercher les compartiments inclus dans votre compte. Si vous choisissez Parcourir S3, choisissez le compartiment souhaité, puis choisissez Choisir un chemin pour renseigner le champ Nom du compartiment avec le nom de ce compartiment.
6. Pour Origine du réseau, choisissez Internet.

   Pour en savoir plus sur les origines de réseau des points d'accès, consultez Création de points d'accès restreints à un virtual private cloud.
7. Par défaut, tous les paramètres de blocage d'accès public sont activés pour votre point d'accès. Nous vous recommandons de conserver l'option Bloquer tous les accès publics activée.

   Pour en savoir plus, consultez Gestion de l'accès public aux points d'accès pour les compartiments à usage général.
8. Pour tous les autres paramètres de point d'accès, conservez les paramètres par défaut.

   (Facultatif) Vous pouvez modifier les paramètres du point d'accès afin de prendre en charge votre cas d'utilisation. Pour ce didacticiel, nous vous recommandons de conserver les paramètres par défaut.

   (Facultatif) Si vous devez gérer l'accès à votre point d'accès, vous pouvez indiquer une politique de point d'accès. Pour plus d'informations, consultez Exemples de politiques pour les points d'accès.
9. Choisissez Créer un point d'accès.

Étape 4 : créer une fonction Lambda

Pour transformer des données originales, créez une fonction Lambda à utiliser avec votre point d'accès S3 Object Lambda.

Sous-étapes

- Écrire le code d'une fonction Lambda et créer un package de déploiement avec un environnement virtuel
- Créer une fonction Lambda à l'aide d'un rôle d'exécution (console)
- Déployez le code de votre fonction Lambda avec les archives du fichier .zip et configurez la fonction Lambda (console)

Écrire le code d'une fonction Lambda et créer un package de déploiement avec un environnement virtuel

1. Sur votre ordinateur local, créez un dossier avec le nom du dossier `object-lambda` afin que l'environnement virtuel puisse l'utiliser ultérieurement dans ce didacticiel.
2. Dans le dossier `object-lambda`, créez un fichier avec une fonction Lambda qui change tout le texte de l'objet original en majuscules. Par exemple, vous pouvez utiliser la fonction suivante écrite en langage Python. Enregistrez cette fonction dans un fichier nommé `transform.py`.

```
import boto3
import requests
from botocore.config import Config

# This function capitalizes all text in the original object
def lambda_handler(event, context):
    object_context = event["getObjectContext"]
    # Get the presigned URL to fetch the requested original object
    # from S3
    s3_url = object_context["inputS3Url"]
    # Extract the route and request token from the input context
    request_route = object_context["outputRoute"]
    request_token = object_context["outputToken"]

    # Get the original S3 object using the presigned URL
    response = requests.get(s3_url)
    original_object = response.content.decode("utf-8")

    # Transform all text in the original object to uppercase
```

```
    # You can replace it with your custom code based on your use case
    transformed_object = original_object.upper()

    # Write object back to S3 Object Lambda
    s3 = boto3.client('s3', config=Config(signature_version='s3v4'))
    # The WriteGetObjectResponse API sends the transformed data
    # back to S3 Object Lambda and then to the user
    s3.write_get_object_response(
        Body=transformed_object,
        RequestRoute=request_route,
        RequestToken=request_token)

    # Exit the Lambda function: return the status code
    return {'status_code': 200}
```

> **Note**
>
> L'exemple précédent de fonction Lambda charge l'ensemble de l'objet demandé en mémoire avant de le transformer et de le renvoyer au client. Vous pouvez autrement diffuser l'objet à partir de S3 pour éviter de charger l'intégralité de l'objet dans la mémoire. Cette approche peut être utile lorsque vous travaillez avec des objets volumineux. Pour en savoir plus sur le streaming des réponses avec des points d'accès Object Lambda, consultez les exemples de streaming dans Utilisation de requêtes `GetObject` dans Lambda.

Lorsque vous écrivez une fonction Lambda à utiliser avec un point d'accès S3 Objet Lambda, la fonction est basée sur le contexte d'événement d'entrée que S3 Object Lambda fournit à la fonction Lambda. Le contexte de l'événement fournit des informations sur la demande effectuée dans l'événement transmis de S3 Object Lambda à Lambda. Il contient les paramètres que vous utiliserez pour créer la fonction Lambda.

Les champs utilisés pour créer la fonction Lambda précédente sont les suivants :

Le champ de `getObjectContext` indique les détails d'entrée et de sortie pour les connexions à Amazon S3 et à S3 Object Lambda. Il comporte les champs suivants :

- `inputS3Url` – Une URL présignée que la fonction Lambda peut utiliser pour télécharger l'objet original à partir du point d'accès de prise en charge. En utilisant une URL présignée, la

fonction Lambda n'a pas besoin des autorisations de lecture Amazon S3 pour récupérer l'objet original et peut uniquement accéder à l'objet traité par chaque invocation.

- `outputRoute` – Un jeton de routage qui est ajouté à l'URL S3 Object Lambda lorsque la fonction Lambda appelle `WriteGetObjectResponse` pour renvoyer l'objet transformé.
- `outputToken` – Un jeton utilisé par S3 Object Lambda pour correspondre à l'appel `WriteGetObjectResponse` avec l'appelant original lors du renvoi de l'objet transformé.

Pour en savoir plus sur tous les champs du contexte de l'événement, consultez Format et utilisation du contexte d'événement et Écriture de fonctions Lambda pour les points d'accès S3 Object Lambda.

3. Dans votre terminal local, saisissez la commande suivante pour installer le package `virtualenv` :

```
python -m pip install virtualenv
```

4. Dans votre terminal local, ouvrez le dossier `object-lambda` que vous avez créé précédemment, puis saisissez la commande suivante pour créer et initialiser un environnement virtuel nommé `venv`.

```
python -m virtualenv venv
```

5. Pour activer l'environnement virtuel, saisissez la commande suivante pour exécuter le fichier `activate` à partir du dossier de l'environnement :

   Pour les utilisateurs macOS, exécutez cette commande :

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

   Pour les utilisateurs Windows, exécutez cette commande :

```
.\venv\Scripts\activate
```

   Votre invite de commande change maintenant pour afficher (venv), indiquant que l'environnement virtuel est actif.

6. Pour installer les bibliothèques requises, exécutez les commandes suivantes ligne par ligne dans l'`venv`environnement virtuel.

Ces commandes installent des versions mises à jour des dépendances de votre `lambda_handler`fonction Lambda. Ces dépendances sont les AWS SDK for Python (Boto3) et le module des demandes.

```
pip3 install boto3
```

```
pip3 install requests
```

7. Pour désactiver l'environnement virtuel, exécutez la commande suivante :

```
deactivate
```

8. Pour créer un package de déploiement avec les bibliothèques installées en tant que fichier `.zip` nommé `lambda.zip` à la racine du répertoire `object-lambda`, exécutez la commande les commandes ligne par ligne dans votre terminal local.

> **Tip**
>
> Les commandes suivantes peuvent nécessiter des ajustements pour fonctionner dans votre environnement particulier. Par exemple, une bibliothèque peut s'afficher dans `site-packages` ou dans `dist-packages`, et le premier dossier peut être `lib` ou `lib64`. En outre, il est possible de nommer le fichier `python` avec une version de Python différente. Vous pouvez utiliser la commande `pip show` pour localiser un package spécifique.

Pour les utilisateurs macOS, exécutez les commandes suivantes :

```
cd venv/lib/python3.8/site-packages
```

```
zip -r ../../../../lambda.zip .
```

Pour les utilisateurs Windows, exécutez les commandes suivantes :

```
cd .\venv\Lib\site-packages\
```

```
powershell Compress-Archive * ../../../lambda.zip
```

La dernière commande enregistre le package de déploiement à la racine du répertoire `object-lambda`.

9. Ajoutez le fichier de code de fonction `transform.py` à la racine de votre package de déploiement.

   Pour les utilisateurs macOS, exécutez les commandes suivantes :

   ```
   cd ../../../../
   ```

   ```
   zip -g lambda.zip transform.py
   ```

   Pour les utilisateurs Windows, exécutez les commandes suivantes :

   ```
   cd ..\..\..\
   ```

   ```
   powershell Compress-Archive -update transform.py lambda.zip
   ```

   Lorsque vous aurez achevé cette étape, vous disposerez de la structure de répertoire suivante :

   ```
   lambda.zip$
     # transform.py
     # __pycache__
     | boto3/
     # certifi/
     # pip/
     # requests/
     ...
   ```

Créer une fonction Lambda à l'aide d'un rôle d'exécution (console)

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.

2. Dans le volet de navigation de gauche, choisissez Fonctions.

3. Choisissez Créer une fonction.
4. Choisissez Créer à partir de zéro.
5. Sous Informations de base, procédez comme suit :

   a. Sous Nom de la fonction, saisissez **`tutorial-object-lambda-function`**.

   b. Pour Exécution, choisissez Python 3.8 ou version ultérieure.
6. Développez la section Changer le rôle d'exécution par défaut. Sous Rôle d'exécution, choisissez Créer un nouveau rôle avec les autorisations Lambda de base.

   À l'étape 5 plus loin dans ce didacticiel, vous associerez AmazonS3 ObjectLambdaExecutionRolePolicy au rôle d'exécution de cette fonction Lambda.
7. Conservez les paramètres restants définis sur les valeurs par défaut.
8. Choisissez Créer une fonction.

Déployez le code de votre fonction Lambda avec les archives du fichier .zip et configurez la fonction Lambda (console)

1. Dans la AWS Lambda console https://console.aws.amazon.com/lambda/, sélectionnez Functions dans le volet de navigation de gauche.
2. Choisissez la fonction Lambda que vous avez créée précédemment (par exemple, **`tutorial-object-lambda-function`**).
3. Dans la page des détails de la fonction Lambda, choisissez l'onglet Code. Dans la section Source du code, choisissez Charger à partir de, puis fichier .zip.
4. Choisissez Charger pour sélectionner votre fichier `.zip` local.
5. Choisissez le fichier `lambda.zip` que vous avez créé précédemment, puis choisissez Ouvrir.
6. Choisissez Enregistrer.
7. Dans la section Paramètres d'exécution, choisissez Modifier.
8. Dans la page Modifier les paramètres d'exécution, confirmez que Exécution est définie sur Python 3.8 ou version ultérieure.
9. Pour indiquer à l'exécution Lambda la méthode de gestionnaire dans votre code de fonction Lambda à invoquer, saisissez **`transform.lambda_handler`** pour Gestionnaire.

   Quand vous configurez une fonction dans Python, la valeur du paramètre de gestionnaire correspond au nom de fichier et au nom de module de gestionnaire, séparés par un point. Par

exemple, `transform.lambda_handler` appelle la méthode `lambda_handler` définie dans le fichier `transform.py`.

10. Choisissez Enregistrer.
11. (Facultatif) Dans la page des détails de votre fonction Lambda, choisissez l'onglet Configuration. Dans le volet de navigation de gauche, choisissez Configuration générale, puis Modifier. Dans le champ Délai d'expiration, saisissez **1** min **0** s. Conservez les paramètres restants définis sur les valeurs par défaut, puis choisissez Enregistrer.

    Le Délai d'expiration est la durée que Lambda autorise pour l'exécution d'une fonction pour invocation avant de l'arrêter. Le durée par défaut est de 3 secondes. La durée maximale d'une fonction Lambda utilisée par S3 Object Lambda est de 60 secondes. La tarification est basée sur la quantité de mémoire configurée et la durée pendant laquelle votre code s'exécute.

Étape 5 : configurer une politique IAM pour le rôle d'exécution de votre fonction Lambda

Pour permettre à votre fonction Lambda de fournir des données personnalisées et des en-têtes de réponse à l'appelant `GetObject`, le rôle d'exécution de votre fonction Lambda doit disposer des autorisations IAM pour appeler l'API `WriteGetObjectResponse`.

Pour attacher une politique IAM au rôle de votre fonction Lambda

1. Dans la AWS Lambda console https://console.aws.amazon.com/lambda/, sélectionnez Functions dans le volet de navigation de gauche.
2. Choisissez la fonction que vous avez créée à l'étape 4 (par exemple, **`tutorial-object-lambda-function`**).
3. Dans la page des détails de votre fonction Lambda, choisissez l'onglet Configuration, puis Autorisations dans le volet de navigation de gauche.
4. Sous Rôle d'exécution, cliquez sur le lien du Nom de rôle. La console IAM s'ouvre.
5. Sur la page Summary (Résumé) de la console IAM pour le rôle d'exécution de votre fonction Lambda, choisissez l'onglet Permissions (Autorisations). Ensuite, dans le menu Add Permissions (Ajouter des autorisations), choisissez Attach policies (Attacher des politiques).
6. Dans la page Attacher des autorisations, saisissez **`AmazonS3ObjectLambdaExecutionRolePolicy`** dans le champ de recherche pour filtrer la liste des politiques. Cochez la case à côté du nom de la politique AmazonS3 ObjectLambdaExecutionRolePolicy.

7. Choisissez Attach Policies (Attacher des politiques).

Étape 6 : créer un point d'accès S3 Object Lambda

Un point d'accès S3 Object Lambda offre la flexibilité d'invoquer une fonction Lambda directement à partir d'une demande GET S3 afin que la fonction puisse traiter les données récupérées à partir d'un point d'accès S3. Lors de la création et de la configuration d'un point d'accès S3 Object Lambda, vous devez indiquer la fonction Lambda à invoquer et fournir le contexte de l'événement au format JSON en tant que paramètres personnalisés à utiliser par Lambda.

Créer un point d'accès S3 Object Lambda

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Dans la page Points d'accès Object Lambda), choisissez Créer un point d'accès Object Lambda).
4. Pour Nom du point d'accès Lambda d'objet, saisissez le nom que vous souhaitez utiliser pour le point d'accès Object Lambda (par exemple, **`tutorial-object-lambda-accesspoint`**).
5. Pour Point d'accès de prise en charge, saisissez ou accédez au point d'accès standard que vous avez créé à l'étape 3 (par exemple, **`tutorial-access-point`**), puis choisissez Choisir un point d'accès de prise en charge.
6. Pour S3 APIs, pour récupérer des objets du compartiment S3 afin que la fonction Lambda les traite, sélectionnez. GetObject
7. Pour invoquer une fonction Lambda, vous pouvez choisir l'une des deux options suivantes de ce didacticiel.
   - Choisissez Choisissez parmi les fonctions dans votre compte, puis choisissez la fonction Lambda que vous avez créée à l'étape 4 (par exemple, **`tutorial-object-lambda-function`**) dans la liste déroulante Fonction Lambda.
   - Choisissez Saisir l'ARN, puis entrez l'Amazon Resource Name (ARN) de la fonction Lambda que vous avez créée à l'étape 4.
8. Pour Version de la fonction Lambda, choisissez $LATEST (la dernière version de la fonction Lambda que vous avez créée à l'étape 4).
9. (Facultatif) Si vous avez besoin de votre fonction Lambda pour reconnaître et traiter les demandes GET avec des en-têtes de plage et de numéro de partie, sélectionnez La fonction

Lambda prend en charge les demandes utilisant la plage et La fonction Lambda prend en charge les demandes utilisant des numéros de partie. Sinon, décochez ces deux cases.

Pour en savoir plus sur l'utilisation des plages ou des numéros de pièce avec S3 Object Lambda, consultez Utilisation des en-têtes Range et partNumber.

10. (Facultatif) Sous Charge utile – facultatif, ajoutez un texte JSON pour fournir des informations supplémentaires à votre fonction Lambda.

    Une charge utile est un texte JSON facultatif que vous pouvez fournir à votre fonction Lambda comme entrée pour toutes les invocations provenant d'un point d'accès S3 Object Lambda spécifique. Pour personnaliser les comportements de plusieurs points d'accès Object Lambda qui invoquent la même fonction Lambda, vous pouvez configurer des charges utiles avec différents paramètres, augmentant ainsi la flexibilité de votre fonction Lambda.

    Pour en savoir plus sur les charges utiles, consultez Format et utilisation du contexte d'événement.

11. (Facultatif) Pour Métriques de demande – facultatif, choisissez Activer ou Désactiver pour ajouter la surveillance Amazon S3 à votre point d'accès Object Lambda. Les statistiques relatives aux demandes sont facturées au CloudWatch tarif standard d'Amazon. Pour en savoir plus, consultez PricingCloudWatch (Tarification).
12. Sous Politique de point d'accès Object Lambda – facultatif, conservez le paramètre par défaut.

    (Facultatif) Vous pouvez définir une politique de ressource. Cette politique de ressource permet à l'autorisation d'API `GetObject` d'utiliser le point d'accès Object Lambda spécifié.

13. Conservez les paramètres restants définis sur les valeurs par défaut, puis choisissez Créer un point d'accès Object Lambda.

Étape 7 : afficher les données transformées

S3 Object Lambda est maintenant prêt à transformer vos données pour votre cas d'utilisation. Dans ce didacticiel, S3 Object Lambda transforme tout le texte de votre objet en majuscules.

Sous-étapes

- Afficher les données transformées dans votre point d'accès S3 Object Lambda
- Exécuter un script Python pour imprimer les données originales et transformées

Afficher les données transformées dans votre point d'accès S3 Object Lambda

Lorsque vous demandez de récupérer un fichier via votre point d'accès S3 Object Lambda, vous effectuez un appel d'API `GetObject` à S3 Object Lambda. S3 Object Lambda invoque la fonction Lambda pour transformer vos données, puis retourne les données transformées en réponse à l'appel d'API `GetObject` S3 standard.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Sur la page Points d'accès Lambda d'objet, choisissez le point d'accès S3 Object Lambda que vous avez créé à l'étape 6 (par exemple, **`tutorial-object-lambda-accesspoint`**).
4. Dans l'onglet Objets de votre point d'accès S3 Object Lambda, sélectionnez le fichier portant le même nom (par exemple, `tutorial.txt`) comme celui que vous avez chargé dans le compartiment S3 à l'étape 2.

   Ce fichier doit contenir toutes les données transformées.
5. Pour afficher les données transformées, choisissez Ouvrir ou Télécharger.

Exécuter un script Python pour imprimer les données originales et transformées

Vous pouvez utiliser S3 Object Lambda avec vos applications existantes. Pour ce faire, mettez à jour la configuration de votre application pour utiliser le nouvel ARN du point d'accès S3 Object Lambda que vous avez créé à l'étape 6 afin de récupérer des données depuis S3.

L'exemple de script Python suivant imprime à la fois les données originales à partir du compartiment S3 et les données transformées à partir du point d'accès S3 Object Lambda.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Sur la page Points d'accès Lambda d'objet, choisissez le bouton radio situé à gauche du point d'accès S3 Object Lambda que vous avez créé à l'étape 6 (par exemple, **`tutorial-object-lambda-accesspoint`**).
4. Choisissez Copier l'ARN.
5. Enregistrez l'ARN pour utilisation ultérieure.

6. Écrivez un script Python sur votre machine locale pour imprimer les données originales (par exemple, `tutorial.txt`) à partir de votre compartiment S3 et les données transformées (par exemple, `tutorial.txt`) à partir de votre point d'accès S3 Object Lambda. Vous pouvez utiliser l'exemple de script suivant.

```
import boto3
from botocore.config import Config

s3 = boto3.client('s3', config=Config(signature_version='s3v4'))

def getObject(bucket, key):
    objectBody = s3.get_object(Bucket = bucket, Key = key)
    print(objectBody["Body"].read().decode("utf-8"))
    print("\n")

print('Original object from the S3 bucket:')
# Replace the two input parameters of getObject() below with
# the S3 bucket name that you created in Step 1 and
# the name of the file that you uploaded to the S3 bucket in Step 2
getObject("tutorial-bucket",
          "tutorial.txt")

print('Object transformed by S3 Object Lambda:')
# Replace the two input parameters of getObject() below with
# the ARN of your S3 Object Lambda Access Point that you saved earlier and
# the name of the file with the transformed data (which in this case is
# the same as the name of the file that you uploaded to the S3 bucket
# in Step 2)
getObject("arn:aws:s3-object-lambda:us-west-2:111122223333:accesspoint/tutorial-
object-lambda-accesspoint",
          "tutorial.txt")
```

7. Enregistrez votre script Python avec un nom personnalisé (par exemple, `tutorial_print.py`) dans le dossier (par exemple, `object-lambda`) que vous avez créé à l'étape 4 sur votre machine locale.

8. Dans votre terminal local, exécutez la commande suivante à partir de la racine du répertoire (par exemple, `object-lambda`) que vous avez créé à l'étape 4.

```
python3 tutorial_print.py
```

Vous devriez voir à la fois les données originales et les données transformées (tout le texte en majuscules) sur le terminal. Par exemple, vous devriez voir quelque chose ressemblant au texte suivant.

```
Original object from the S3 bucket:
Amazon S3 Object Lambda Tutorial:
You can add your own code to process data retrieved from S3 before
returning it to an application.

Object transformed by S3 Object Lambda:
AMAZON S3 OBJECT LAMBDA TUTORIAL:
YOU CAN ADD YOUR OWN CODE TO PROCESS DATA RETRIEVED FROM S3 BEFORE
RETURNING IT TO AN APPLICATION.
```

Étape 8 : nettoyer

Si vous avez transformé vos données via S3 Object Lambda comme un simple exercice d'apprentissage, supprimez les ressources AWS que vous avez allouées afin de ne plus accumuler de frais.

Sous-étapes

- Supprimer le point d'accès Object Lambda
- Supprimer le point d'accès S3
- Supprimer le rôle d'exécution de votre fonction Lambda.
- Supprimer la fonction Lambda
- Supprimer le groupe de CloudWatch journaux
- Supprimer le fichier original dans le compartiment source S3
- Supprimer le compartiment source S3
- Supprimer l'utilisateur IAM

Supprimer le point d'accès Object Lambda

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Points d'accès Object Lambda.

3. Sur la page Points d'accès Lambda d'objet, choisissez le bouton radio situé à gauche du point d'accès S3 Object Lambda que vous avez créé à l'étape 6 (par exemple, **`tutorial-object-lambda-accesspoint`**).
4. Choisissez Supprimer.
5. Confirmez que vous souhaitez supprimer votre point d'accès Object Lambda en saisissant son nom dans le champ de texte qui s'affiche, puis choisissez Supprimer.

Supprimer le point d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Points d'accès.
3. Accédez au point d'accès que vous avez créé à l'étape 3 (par exemple, **`tutorial-access-point`**), puis choisissez le bouton radio en regard du nom du point d'accès.
4. Choisissez Supprimer.
5. Confirmez que vous souhaitez supprimer votre point d'accès Object Lambda en saisissant son nom dans le champ de texte qui s'affiche, puis choisissez Supprimer.

Supprimer le rôle d'exécution de votre fonction Lambda.

1. Connectez-vous à la AWS Lambda console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le panneau de navigation de gauche, choisissez Fonctions.
3. Choisissez la fonction que vous avez créée à l'étape 4 (par exemple, **`tutorial-object-lambda-function`**).
4. Dans la page des détails de votre fonction Lambda, choisissez l'onglet Configuration, puis Autorisations dans le volet de navigation de gauche.
5. Sous Rôle d'exécution, cliquez sur le lien du Nom de rôle. La console IAM s'ouvre.
6. Dans la page Récapitulatif de la console IAM du rôle d'exécution de votre fonction Lambda, choisissez Supprimer le rôle.
7. Dans la boîte de dialogue Supprimer le rôle, choisissez Oui, supprimer.

Supprimer la fonction Lambda

1. Dans la AWS Lambda console https://console.aws.amazon.com/lambda/, sélectionnez Functions dans le volet de navigation de gauche.
2. Cochez la case à gauche du nom de la fonction que vous avez créée à l'étape 4 (par exemple, **`tutorial-object-lambda-function`**).
3. Choisissez Actions, puis Supprimer.
4. Dans la boîte de dialogue Supprimer une fonction, choisissez Supprimer.

Supprimer le groupe de CloudWatch journaux

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation de gauche, choisissez Groupes de journaux.
3. Recherchez le groupe de journaux dont le nom se termine par la fonction Lambda que vous avez créée à l'étape 4 (par exemple, **`tutorial-object-lambda-function`**).
4. Cochez la case située à gauche du nom du groupe de journaux.
5. Choisissez Actions, puis Supprimer le ou les groupes de journaux.
6. Dans la boîte de dialogue Supprimer le ou les groupes de journaux, choisissez Supprimer.

Supprimer le fichier original dans le compartiment source S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Nom du compartiment, choisissez le nom du compartiment vers lequel vous avez chargé le fichier original à l'étape 2 (par exemple, **`tutorial-bucket`**).
4. Cochez la case située à gauche du nom de l'objet que vous souhaitez supprimer (par exemple, `tutorial.txt`).
5. Choisissez Supprimer.
6. Dans la page Supprimer des objets, dans la section Supprimer définitivement les objets ?, confirmez que vous souhaitez supprimer cet objet en saisissant **`permanently delete`** dans la zone de texte.
7. Choisissez Supprimer les objets.

Supprimer le compartiment source S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le bouton radio en regard du nom du compartiment que vous avez créé à l'étape 1 (par exemple, **`tutorial-bucket`**).
4. Choisissez Supprimer.
5. Dans la page Supprimer le compartiment, confirmez que vous souhaitez supprimer le compartiment en saisissant le nom de ce dernier dans le champ de texte, puis choisissez Supprimer le compartiment.

Supprimer l'utilisateur IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation, choisissez Utilisateurs, puis cochez la case en regard du nom de l'utilisateur à supprimer.
3. En haut de la page, choisissez Supprimer.
4. Dans le champ Supprimer ***`user name`*** ? boîte de dialogue, entrez le nom d'utilisateur dans le champ de saisie de texte pour confirmer la suppression de l'utilisateur. Choisissez Supprimer.

Étapes suivantes

Après avoir terminé ce didacticiel, vous pourrez personnaliser la fonction Lambda pour votre cas d'utilisation afin de modifier les données renvoyées par des demandes GET S3 standard.

Voici une liste de cas d'utilisation courants pour S3 Object Lambda :

- Masquer les données sensibles à des fins de sécurité et de conformité.

  Pour plus d'informations, consultez Didacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend.
- Filtrer certaines lignes de données pour fournir des informations précises.
- Enrichir les données avec des informations provenant d'autres services ou bases de données.

- Conversion entre les formats de données, comme la conversion XML en JSON pour la compatibilité des applications.
- Compression ou décompression des fichiers pendant qu'ils sont téléchargés.
- Redimensionnement des images et insertion d'un filigrane.

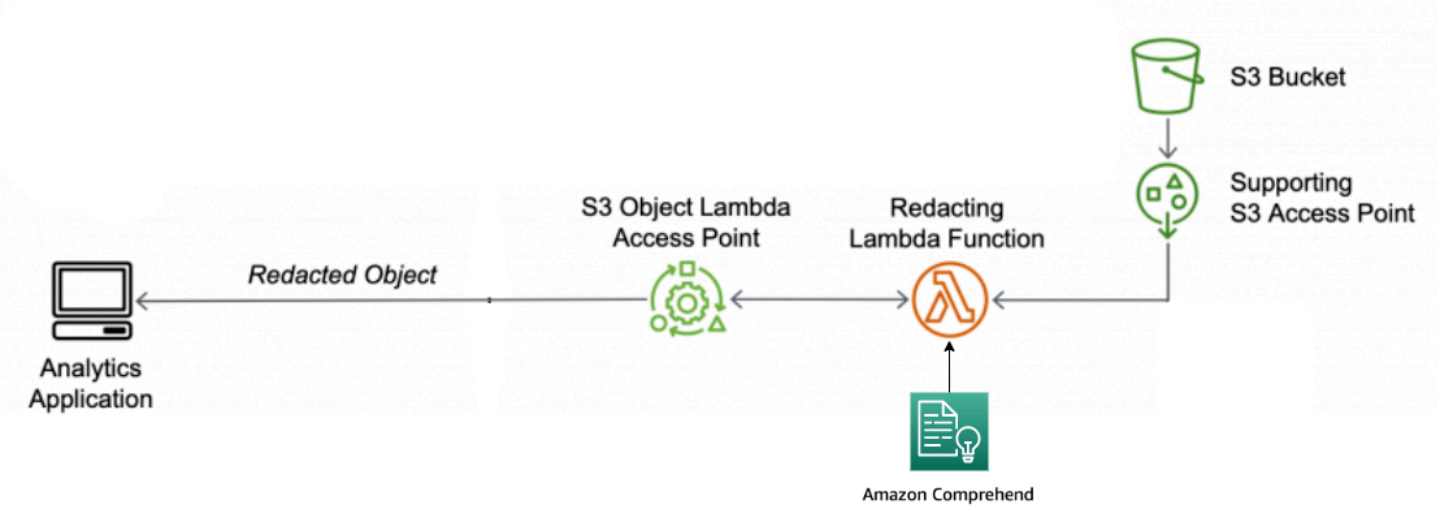
  Pour plus d'informations, consultez Didacticiel : Utilisation de S3 Object Lambda pour filigraner dynamiquement des images au fur et à mesure de leur récupération.
- Mise en œuvre de règles d'autorisation personnalisées pour accéder aux données.

Pour en savoir plus sur S3 Object Lambda, consultez Transformation d'objets avec S3 Object Lambda.

Didacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend

Lorsque vous utilisez Amazon S3 pour des jeux de données partagés auxquels plusieurs applications et utilisateurs peuvent accéder, il est important de restreindre les informations privilégiées, telles que les données d'identification personnelle (PII), aux entités autorisées uniquement. Par exemple, lorsqu'une application marketing utilise des données contenant des DPI, elle doit d'abord masquer les DPI pour répondre aux exigences de confidentialité des données. En outre, lorsqu'une application d'analyse utilise un jeu de données d'inventaire d'ordre de production, elle peut devoir d'abord effacer les informations de carte de crédit du client afin d'éviter toute fuite de données involontaire.

Grâce à S3 Object Lambda et une fonction AWS Lambda optimisée par Amazon Comprehend, vous pouvez protéger les DPI récupérées à partir de S3 avant de les renvoyer à une application. Plus précisément, vous pouvez utiliser la fonction Lambda préconstruite en tant que fonction d'expurgation et l'attacher à un point d'accès S3 Object Lambda. Lorsqu'une application (par exemple, une application d'analyse) envoie des requêtes S3 GET standard, ces demandes effectuées via le point d'accès S3 Object Lambda invoquent la fonction Lambda de rédaction prédéfinie pour détecter et supprimer les données PII extraites d'une source de données sous-jacente via un point d'accès S3 compatible. Ensuite, le point d'accès S3 Object Lambda retourne le résultat expurgé à l'application.



Dans le processus, la fonction Lambda préconstruite utilise Amazon Comprehend, un service de traitement du langage naturel (NLP), qui permet de saisir les variations dans la façon dont les DPI sont représentées, quelle que soit la façon dont les DPI existent dans le texte (par exemple, numériquement ou sous forme de combinaison de mots et de chiffres). Amazon Comprehend peut même utiliser le contexte dans le texte pour comprendre si un numéro à 4 chiffres est un code PIN, les quatre derniers numéros d'un numéro de sécurité sociale (NSS) ou une année. Amazon Comprehend traite n'importe quel fichier texte au format UTF-8 et peut protéger les DPI à grande échelle sans affecter la précision. Pour plus d'informations, consultez Qu'est-ce qu'Amazon Comprehend ? dans le guide du développeur Amazon Comprehend.

Objectif

Dans ce didacticiel, vous apprendrez à utiliser S3 Object Lambda avec la fonction Lambda préconstruite `ComprehendPiiRedactionS3ObjectLambda`. Cette fonction utilise Amazon Comprehend pour détecter les entités DPI. Elle supprime ensuite ces entités en les remplaçant par des astérisques. En expurgeant des DPI, vous masquez les données sensibles, ce qui peut aider en matière de sécurité et de conformité.

Vous apprendrez également à utiliser et à configurer une AWS Lambda fonction prédéfinie dans le AWS Serverless Application Repositorypour qu'elle fonctionne avec S3 Object Lambda afin de faciliter le déploiement.

Rubriques

- Conditions préalables : Créer un utilisateur IAM avec des autorisations
- Étape 1 : Créer un compartiment S3
- Étape 2 : charger un fichier dans le compartiment S3

- Étape 3 : créer un point d'accès S3
- Étape 4 : configurer et déployer une fonction Lambda préconstruite
- Étape 5 : créer un point d'accès S3 Object Lambda
- Étape 6 : utiliser le point d'accès S3 Object Lambda pour récupérer le fichier expurgé
- Étape 7 : nettoyer
- Étapes suivantes

Conditions préalables : Créer un utilisateur IAM avec des autorisations

Avant de commencer ce didacticiel, vous devez disposer d'un AWS compte auquel vous pouvez vous connecter en tant qu' AWS Identity and Access Management utilisateur (utilisateur IAM) avec les autorisations appropriées.

Vous pouvez créer un utilisateur IAM pour le didacticiel. Pour terminer ce didacticiel, votre utilisateur IAM doit joindre les politiques IAM suivantes pour accéder aux AWS ressources pertinentes et effectuer des actions spécifiques.

> **Note**
>
> Pour des raisons de simplicité, ce didacticiel crée et utilise un utilisateur IAM. Après avoir terminé ce didacticiel, n'oubliez pas de Supprimer l'utilisateur IAM. Pour une utilisation en production, nous vous recommandons de suivre les Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM. Une bonne pratique requiert que les utilisateurs humains utilisent une fédération avec un fournisseur d'identité pour accéder à AWS avec des informations d'identification temporaires. Une autre bonne pratique consiste à exiger que les charges de travail utilisent des informations d'identification temporaires avec des rôles IAM pour accéder à AWS. Pour en savoir plus sur l'utilisation AWS IAM Identity Center pour créer des utilisateurs avec des informations d'identification temporaires, voir Getting started dans le guide de AWS IAM Identity Center l'utilisateur.
> Pour plus de simplicité, ce didacticiel utilise des stratégies d'accès complet. Pour utilisation en production, nous vous recommandons d'accorder uniquement les autorisations minimales nécessaires à votre cas d'utilisation, conformément aux Bonnes pratiques de sécurité.

Votre utilisateur IAM a besoin des politiques AWS gérées suivantes :

- AmazonS3 FullAccess — Accorde des autorisations pour toutes les actions Amazon S3, y compris les autorisations pour créer et utiliser un point d'accès Object Lambda.
- AWSLambda_FullAccess— Accorde des autorisations à toutes les actions Lambda.
- AWSCloudFormationFullAccess— Accorde des autorisations pour toutes les AWS CloudFormation actions.
- IAMFullAccès : accorde des autorisations à toutes les actions IAM.
- IAMAccessAnalyzerReadOnlyAccess— Accorde l'autorisation de lire toutes les informations d'accès fournies par IAM Access Analyzer.

Vous pouvez attacher directement ces politiques existantes lors de la création d'un utilisateur IAM. Pour en savoir plus sur la création d'un utilisateur IAM, consultez Créer votre premier groupe d'utilisateurs et d'administrateurs IAM dans le guide de l'utilisateur IAM.

En outre, votre utilisateur IAM nécessite une politique gérée par le client. Pour accorder à l'utilisateur IAM des autorisations sur toutes les AWS Serverless Application Repository ressources et actions, vous devez créer une stratégie IAM et l'associer à l'utilisateur IAM.

Créer et attacher une politique IAM à votre utilisateur IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de gauche, choisissez Politiques.
3. Choisissez Créer une politique.
4. Dans l'onglet Éditeur visuel, pour Service, choisissez Choisir un service. Ensuite, choisissez Serverless Application Repository.
5. Pour Actions, sous Actions manuelles, sélectionnez Toutes les actions du Serverless Application Repository (serverlessrepo :*) pour ce didacticiel.

   En tant que bonne pratique de sécurité, vous devez autoriser un utilisateur à accéder uniquement aux actions et ressources qui lui sont nécessaires, selon votre cas d'utilisation. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.
6. Pour Ressources, choisissez Toutes les ressources pour ce didacticiel.

   La bonne pratique consiste à définir des autorisations pour des ressources spécifiques uniquement dans des comptes spécifiques. Vous pouvez autrement accorder le moindre

privilège en utilisant des clés de condition. Pour plus d'informations, consultez Accorder le moindre privilège dans le guide de l'utilisateur IAM.

7. Choisissez Suivant : Balises.
8. Choisissez Suivant : Vérification.
9. Dans la page Examiner une politique, saisissez un nom (par exemple, **`tutorial-serverless-application-repository`**) et une Description (facultatif) pour la politique que vous êtes en train de créer. Examinez le récapitulatif de la politique afin de vérifier que vous avez accordé les autorisations souhaitées, puis choisissez Créer une politique pour enregistrer votre nouvelle politique.
10. Dans le volet de navigation de gauche, choisissez Utilisateurs. Ensuite, choisissez l'utilisateur IAM pour ce didacticiel.
11. Dans la page Récapitulatif de l'utilisateur sélectionné, choisissez l'onglet Autorisations, puis choisissez Ajouter des autorisations.
12. Sous Octroyer des autorisations, choisissez Attacher directement les politiques existantes.
13. Cochez la case en regard de la politique que vous avez créée (par exemple, **`tutorial-serverless-application-repository`**), puis choisissez Suivant : Examiner.
14. Sous Récapitulatif des autorisations, examinez le récapitulatif de la politique afin de vérifier que vous avez attaché la politique prévue. Choisissez ensuite Ajouter des autorisations.

Étape 1 : Créer un compartiment S3

Créez un compartiment pour stocker les données originales que vous prévoyez de transformer.

> **Note**
>
> Des points d'accès peuvent être attachés à une autre source de données, telle qu'un volume Amazon FSx pour OpenZFS, mais ce didacticiel utilise un point d'accès auxiliaire attaché à un compartiment S3.

Pour créer un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Choisissez Créer un compartiment.

La page Créer un compartiment s'ouvre.

4. Pour Nom du compartiment, saisissez un nom (par exemple, **`tutorial-bucket`**) pour votre compartiment.

   Pour en savoir plus sur les règles d'attribution de noms des compartiments Amazon S3, consultez Règles de dénomination des compartiments à usage général.

5. Dans Région, choisissez la Région AWS dans laquelle le compartiment doit résider.

   Pour en savoir plus sur les régions des compartiments, consultez Présentation des compartiments à usage général.

6. Pour Paramètres de blocage de l'accès public à ce compartiment, conservez les paramètres par défaut (Bloquer tout accès public est activé).

   Nous vous recommandons de laisser tous les paramètres de blocage de l'accès public activés, sauf si vous devez en désactiver un ou plusieurs pour votre cas d'utilisation. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

7. Pour les paramètres restants, conservez les paramètres par défaut.

   (Facultatif) Si vous souhaitez configurer des paramètres de compartiment supplémentaires pour votre cas d'utilisation particulier, consultez Création d'un bucket à usage général.

8. Choisissez Créer un compartiment.

Étape 2 : charger un fichier dans le compartiment S3

Téléchargez un fichier texte contenant des données personnelles connues de différents types, telles que des noms, des informations bancaires, des numéros de téléphone SSNs, et dans le compartiment S3 en tant que données d'origine dont vous supprimerez les informations personnelles ultérieurement dans ce didacticiel.

Par exemple, vous pouvez charger le fichier `tutorial.txt` suivant. Voici un exemple de fichier d'entrée Amazon Comprehend.

```
Hello Zhang Wei, I am John. Your AnyCompany Financial Services,
LLC credit card account 1111-0000-1111-0008 has a minimum payment
of $24.53 that is due by July 31st. Based on your autopay settings,
we will withdraw your payment on the due date from your
```

```
bank account number XXXXXX1111 with the routing number XXXXX0000.

Your latest statement was mailed to 100 Main Street, Any City,
WA 98121.
After your payment is received, you will receive a confirmation
text message at 206-555-0100.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at 206-555-0199 or
email at support@anycompany.com.
```

Charger un fichier dans un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment que vous avez créé à l'étape 1 (par exemple, **`tutorial-bucket`**) pour y charger votre fichier.
4. Sous l'onglet Objets de votre compartiment, choisissez Charger.
5. Dans la page Charger, sous Fichiers et dossiers, choisissez Ajouter des fichiers.
6. Choisissez un fichier à charger, puis choisissez Ouvrir. Par exemple, vous pouvez charger le fichier `tutorial.txt` mentionné précédemment.
7. Choisissez Charger.

Étape 3 : créer un point d'accès S3

Pour utiliser un point d'accès S3 Object Lambda afin d'accéder aux données originales et de les transformer, vous devez créer un point d'accès S3 et l'associer au compartiment S3 que vous avez créé à l'étape 1. Le point d'accès doit se trouver dans le même Région AWS emplacement que les objets que vous souhaitez transformer.

Plus loin dans ce didacticiel, vous utiliserez ce point d'accès comme point d'accès de prise en charge pour votre point d'accès Object Lambda.

Créer un point d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Points d'accès.

3. Dans la page Points d'accès, choisissez Créer un point d'accès.
4. Dans le champ Nom du point d'accès, saisissez le nom (par exemple, **`tutorial-pii-access-point`**) du point d'accès.

   Pour en savoir plus sur l'attribution de noms aux points d'accès, consultez Règles de dénomination pour les points d'accès.
5. Dans le champ Source de données, entrez le nom du bucket que vous avez créé à l'étape 1 (par exemple,**`tutorial-bucket`**). S3 attache le point d'accès à ce compartiment.

   (Facultatif) Vous pouvez choisir Parcourir S3 pour parcourir et rechercher les compartiments inclus dans votre compte. Si vous choisissez Parcourir S3, choisissez le compartiment souhaité, puis choisissez Choisir un chemin pour renseigner le champ Nom du compartiment avec le nom de ce compartiment.
6. Pour Origine du réseau, choisissez Internet.

   Pour en savoir plus sur les origines de réseau des points d'accès, consultez Création de points d'accès restreints à un virtual private cloud.
7. Par défaut, tous les paramètres de blocage d'accès public sont activés pour votre point d'accès. Nous vous recommandons de conserver l'option Bloquer tous les accès publics activée. Pour en savoir plus, consultez Gestion de l'accès public aux points d'accès pour les compartiments à usage général.
8. Pour tous les autres paramètres de point d'accès, conservez les paramètres par défaut.

   (Facultatif) Vous pouvez modifier les paramètres du point d'accès afin de prendre en charge votre cas d'utilisation. Pour ce didacticiel, nous vous recommandons de conserver les paramètres par défaut.

   (Facultatif) Si vous devez gérer l'accès à votre point d'accès, vous pouvez indiquer une politique de point d'accès. Pour plus d'informations, consultez Exemples de politiques pour les points d'accès.
9. Choisissez Créer un point d'accès.

Étape 4 : configurer et déployer une fonction Lambda préconstruite

Pour effacer les DPI, configurez et déployez la fonction AWS Lambda `ComprehendPiiRedactionS3ObjectLambda` préconstruite à utiliser avec votre point d'accès S3 Object Lambda.

Configurez et déployez la fonction Lambda

1. Connectez-vous au AWS Management Console et visualisez la `ComprehendPiiRedactionS3ObjectLambda`fonction dans le AWS Serverless Application Repository.
2. Pour les Paramètres de l'application, sous Nom de l'application, conservez la valeur par défaut (`ComprehendPiiRedactionS3ObjectLambda`) pour ce didacticiel.

   (Facultatif) Vous pouvez saisir le nom que vous souhaitez donner à cette application. Vous pouvez faire ceci si vous prévoyez de configurer plusieurs fonctions Lambda pour différents besoins d'accès au même jeu de données partagé.
3. Pour MaskCharacter, conservez la valeur par défaut (*****). Le caractère de masque remplace chaque caractère de l'entité DPI expurgée.
4. Pour MaskMode, conservez la valeur par défaut (MASK). La MaskModevaleur indique si l'entité PII est expurgée avec le `MASK` caractère ou la `PII_ENTITY_TYPE` valeur.
5. Pour supprimer les types de données spécifiés, pour PiiEntityTypes, conservez la valeur par défaut ALL. La PiiEntityTypesvaleur indique les types d'entités PII à prendre en compte pour la rédaction.

   Pour en savoir plus sur la liste des types d'entités DPI pris en charge, consultez Détecter les données d'identification personnelle (PII) dans le guide du développeur Amazon Comprehend.
6. Conservez les paramètres restants définis sur les valeurs par défaut.

   (Facultatif) Si vous souhaitez configurer des paramètres supplémentaires pour votre cas d'utilisation spécifique, consultez la section Fichier Readme sur le côté gauche de la page.
7. Cochez la case en regard de Je reconnais que cette application crée des rôles IAM personnalisés.
8. Choisissez Déployer.
9. Dans la page de la nouvelle application, sous Ressources, choisissez l'ID logique de la fonction Lambda que vous avez déployée pour examiner la fonction dans la page de la fonction Lambda.

Étape 5 : créer un point d'accès S3 Object Lambda

Un point d'accès S3 Object Lambda offre la flexibilité d'invoquer une fonction Lambda directement à partir d'une demande GET S3 afin que la fonction puisse supprimer les DPI récupérées à partir d'un point d'accès S3. Lors de la création et de la configuration d'un point d'accès S3 Object Lambda,

vous devez indiquer la fonction d'expurgation Lambda à invoquer et fournir le contexte d'événement au format JSON en tant que paramètres personnalisés pour utilisation par Lambda.

Le contexte d'événement fournit des informations sur la demande effectuée dans l'événement transmis de S3 Object Lambda à Lambda. Pour en savoir plus sur tous les champs du contexte d'événement, consultez Format et utilisation du contexte d'événement.

Créer un point d'accès S3 Object Lambda

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Dans la page Points d'accès Object Lambda), choisissez Créer un point d'accès Object Lambda).
4. Pour Nom du point d'accès Lambda d'objet, saisissez le nom que vous souhaitez utiliser pour le point d'accès Object Lambda (par exemple, **`tutorial-pii-object-lambda-accesspoint`**).
5. Pour Point d'accès de prise en charge, saisissez ou accédez au point d'accès standard que vous avez créé à l'étape 3 (par exemple, **`tutorial-pii-access-point`**), puis choisissez Choisir un point d'accès de prise en charge.
6. Pour S3 APIs, pour récupérer des objets du compartiment S3 afin que la fonction Lambda les traite, sélectionnez. GetObject
7. Pour Appeler une fonction Lambda, vous pouvez choisir l'une des deux options suivantes pour ce didacticiel.
   - Choisissez Choisir parmi les fonctions de votre compte et choisissez la fonction Lambda que vous avez déployée à l'étape 4 (par exemple, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**) dans la liste déroulante Fonction Lambda.
   - Choisissez Saisir l'ARN, puis saisissez l'Amazon Resource Name (ARN) de la fonction Lambda que vous avez créée à l'étape 4.
8. Pour Version de la fonction Lambda, choisissez $LATEST (la dernière version de la fonction Lambda que vous avez déployée à l'étape 4).
9. (Facultatif) Si vous avez besoin de votre fonction Lambda pour reconnaître et traiter les demandes GET avec des en-têtes de plage et de numéro de partie, sélectionnez La fonction Lambda prend en charge les demandes utilisant la plage et La fonction Lambda prend en charge les demandes utilisant des numéros de partie. Sinon, décochez ces deux cases.

Pour en savoir plus sur l'utilisation des plages ou des numéros de pièce avec S3 Object Lambda, consultez Utilisation des en-têtes Range et partNumber.

10. (Facultatif) Sous Charge utile – facultatif, ajoutez un texte JSON pour fournir des informations supplémentaires à votre fonction Lambda.

    Une charge utile est un texte JSON facultatif que vous pouvez fournir à votre fonction Lambda comme entrée pour toutes les invocations provenant d'un point d'accès S3 Object Lambda spécifique. Pour personnaliser les comportements de plusieurs points d'accès Object Lambda qui invoquent la même fonction Lambda, vous pouvez configurer des charges utiles avec différents paramètres, augmentant ainsi la flexibilité de votre fonction Lambda.

    Pour en savoir plus sur les charges utiles, consultez Format et utilisation du contexte d'événement.

11. (Facultatif) Pour Métriques de demande – facultatif, choisissez Activer ou Désactiver pour ajouter la surveillance Amazon S3 à votre point d'accès Object Lambda. Les statistiques relatives aux demandes sont facturées au CloudWatch tarif standard d'Amazon. Pour en savoir plus, consultez PricingCloudWatch (Tarification).
12. Sous Politique de point d'accès Object Lambda – facultatif, conservez le paramètre par défaut.

    (Facultatif) Vous pouvez définir une politique de ressource. Cette politique de ressource permet à l'autorisation d'API `GetObject` d'utiliser le point d'accès Object Lambda spécifié.

13. Conservez les paramètres restants définis sur les valeurs par défaut, et choisissez Créer un point d'accès Object Lambda.

Étape 6 : utiliser le point d'accès S3 Object Lambda pour récupérer le fichier expurgé

Maintenant, S3 Object Lambda est prêt à expurger les DPI de votre fichier original.

Pour utiliser le point d'accès S3 Object Lambda pour récupérer le fichier expurgé

Lorsque vous demandez de récupérer un fichier via votre point d'accès S3 Object Lambda, vous effectuez un appel d'API `GetObject` à S3 Object Lambda. L'objet S3 Lambda invoque la fonction Lambda pour expurger vos DPI et retourne les données transformées comme réponse à l'appel d'API`GetObject` S3 standard.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le panneau de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Sur la page Points d'accès Lambda d'objet, choisissez le point d'accès S3 Object Lambda que vous avez créé à l'étape 5 (par exemple, **`tutorial-pii-object-lambda-accesspoint`**).
4. Dans l'onglet Objets de votre point d'accès S3 Object Lambda, sélectionnez le fichier portant le même nom (par exemple, `tutorial.txt`) comme celui que vous avez chargé dans le compartiment S3 à l'étape 2.

   Ce fichier doit contenir toutes les données transformées.
5. Pour afficher les données transformées, choisissez Ouvrir ou Télécharger.

   Vous devriez pouvoir voir le fichier expurgé, comme illustré dans l'exemple suivant.

```
Hello *********. Your AnyCompany Financial Services,
LLC credit card account ******************* has a minimum payment
of $24.53 that is due by *********. Based on your autopay settings,
we will withdraw your payment on the due date from your
bank account ********** with the routing number *********.

Your latest statement was mailed to ********************************.
After your payment is received, you will receive a confirmation
text message at ************.
If you have questions about your bill, AnyCompany Customer Service
is available by phone at ************ or
email at **********************.
```

Étape 7 : nettoyer

Si vous avez expurgé vos données via S3 Object Lambda uniquement à des fins d'apprentissage, supprimez AWS les ressources que vous avez allouées afin de ne plus payer de frais.

Sous-étapes

- Supprimer le point d'accès Object Lambda
- Supprimer le point d'accès S3
- Supprimer la fonction Lambda
- Supprimer le groupe de CloudWatch journaux
- Supprimer le fichier original dans le compartiment source S3

- Supprimer le compartiment source S3
- Supprimer le rôle IAM de votre fonction Lambda
- Supprimer la politique gérée par le client de votre utilisateur IAM
- Supprimer l'utilisateur IAM

Supprimer le point d'accès Object Lambda

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Points d'accès Object Lambda.
3. Sur la page Points d'accès Lambda d'objet, choisissez le bouton d'option situé à gauche du point d'accès S3 Object Lambda que vous avez créé à l'étape 5 (par exemple, **`tutorial-pii-object-lambda-accesspoint`**).
4. Choisissez Supprimer.
5. Confirmez que vous souhaitez supprimer votre point d'accès Object Lambda en saisissant son nom dans le champ de texte qui s'affiche, puis choisissez Supprimer.

Supprimer le point d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation, choisissez Points d'accès.
3. Accédez au point d'accès que vous avez créé à l'étape 3 (par exemple, **`tutorial-pii-access-point`**) et choisissez le bouton d'option en regard du nom du point d'accès.
4. Choisissez Supprimer.
5. Confirmez que vous souhaitez supprimer votre point d'accès en saisissant son nom dans le champ de texte qui s'affiche, puis choisissez Supprimer.

Supprimer la fonction Lambda

1. Dans la AWS Lambda console https://console.aws.amazon.com/lambda/, sélectionnez Functions dans le volet de navigation de gauche.
2. Choisissez la fonction que vous avez créée à l'étape 4 (par exemple, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**).

3. Choisissez Actions, puis choisissez Supprimer.
4. Dans la boîte de dialogue Supprimer une fonction, choisissez Supprimer.

Supprimer le groupe de CloudWatch journaux

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation de gauche, choisissez Groupes de journaux.
3. Recherchez le groupe de journaux dont le nom se termine par la fonction Lambda que vous avez créée à l'étape 4 (par exemple, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**).
4. Choisissez Actions, puis choisissez Supprimer le groupe de journaux.
5. Dans la boîte de dialogue Supprimer le ou les groupes de journaux, choisissez Supprimer.

Supprimer le fichier original dans le compartiment source S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Nom du compartiment, choisissez le nom du compartiment vers lequel vous avez chargé le fichier original à l'étape 2 (par exemple, **`tutorial-bucket`**).
4. Cochez la case située à gauche du nom de l'objet que vous souhaitez supprimer (par exemple, `tutorial.txt`).
5. Choisissez Supprimer.
6. Dans la page Supprimer des objets, dans la section Supprimer définitivement les objets ?, confirmez que vous souhaitez supprimer cet objet en saisissant **`permanently delete`** dans la zone de texte.
7. Choisissez Supprimer les objets.

Supprimer le compartiment source S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.

3. Dans la liste Compartiments, choisissez le bouton d'option en regard du nom du compartiment que vous avez créé à l'étape 1 (par exemple, **`tutorial-bucket`**).
4. Choisissez Supprimer.
5. Dans la page Supprimer un compartiment, confirmez que vous souhaitez supprimer le compartiment en saisissant le nom du compartiment dans le champ de texte, puis choisissez Supprimer un compartiment.

Supprimer le rôle IAM de votre fonction Lambda

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de gauche, choisissez Rôles, puis cochez la case en regard du rôle à supprimer. Le nom du rôle commence par le nom de la fonction Lambda que vous avez déployée à l'étape 4 (par exemple, **`serverlessrepo-ComprehendPiiRedactionS3ObjectLambda`**).
3. Choisissez Supprimer.
4. Dans la boîte de dialogue Supprimer, saisissez le nom du rôle dans le champ de saisie de texte pour confirmer la suppression. Ensuite, choisissez Supprimer.

Supprimer la politique gérée par le client de votre utilisateur IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation de gauche, choisissez Politiques.
3. Dans la page Politiques, saisissez le nom de la politique gérée par le client que vous avez créée dans les conditions préalables (par exemple, **`tutorial-serverless-application-repository`**) dans la zone de recherche pour filtrer la liste des politiques. Sélectionnez le bouton d'option en regard du nom de la politique à supprimer.
4. Choisissez Actions, puis choisissez Supprimer.
5. Confirmez que vous souhaitez supprimer cette politique en saisissant son nom dans le champ de texte qui s'affiche, puis choisissez Supprimer.

Supprimer l'utilisateur IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation, choisissez Utilisateurs, puis cochez la case en regard du nom de l'utilisateur à supprimer.
3. En haut de la page, choisissez Supprimer.
4. Dans le champ Supprimer ***user name*** ? boîte de dialogue, entrez le nom d'utilisateur dans le champ de saisie de texte pour confirmer la suppression de l'utilisateur. Choisissez Supprimer.

Étapes suivantes

Après avoir terminé ce didacticiel, vous pouvez explorer plus en détail les cas d'utilisation connexes suivants :

- Vous pouvez créer plusieurs points d'accès S3 Lambda Object et les activer avec des fonctions Lambda préconstruites qui sont configurées différemment pour expurger des types spécifiques de DPI en fonction des besoins métier des accesseurs aux données.

  Chaque type d'utilisateur assume un rôle IAM et n'a accès qu'à un seul point d'accès S3 Object Lambda (géré via des politiques IAM). Ensuite, vous attachez chaque fonction Lambda `ComprehendPiiRedactionS3ObjectLambda` configurée pour un cas d'utilisation d'expurgation différent à un autre point d'accès S3 Object Lambda. Pour chaque point d'accès S3 Object Lambda, vous pouvez disposer d'un point d'accès S3 prenant en charge la lecture des données à partir d'un compartiment S3 qui stocke le jeu de données partagé.

  Pour en savoir plus sur la façon de créer une politique de compartiment S3 qui permet aux utilisateurs de lire à partir du compartiment uniquement via des points d'accès S3, consultez Configuration des politiques IAM pour l'utilisation des points d'accès.

  Pour en savoir plus sur la façon d'octroyer à un utilisateur l'autorisation d'accéder à la fonction Lambda, au point d'accès S3 et au point d'accès S3 Object Lambda, consultez Configuration des politiques IAM pour les points d'accès Object Lambda.
- Vous pouvez créer votre propre fonction Lambda et utiliser S3 Object Lambda avec votre fonction Lambda personnalisée pour répondre à vos besoins spécifiques en matière de données.

  Par exemple, pour explorer diverses valeurs de données, vous pouvez utiliser S3 Object Lambda et votre propre fonction Lambda qui utilise des fonctions Amazon Comprehend, telles que

la reconnaissance des entités, la reconnaissance des mots clés, l'analyse du ressenti et la classification des documents, pour traiter les données. Vous pouvez également utiliser S3 Object Lambda avec Amazon Comprehend Medical, un service NLP admissible à HIPAA, pour analyser et extraire des données d'une manière contextuelle.

Pour en savoir plus sur la façon de transformer des données avec S3 Object Lambda et votre propre fonction Lambda, consultez Didacticiel : Transformation de données pour votre application avec S3 Object Lambda.

Débogage et résolution des problèmes de S3 Object Lambda

Les demandes adressées aux points d'accès S3 Object Lambda peuvent entraîner une nouvelle réponse d'erreur en cas de problème avec l'invocation ou l'exécution de la fonction Lambda. Ces erreurs respectent le même format que les erreurs Amazon S3 standard. Pour plus d'informations sur les erreurs S3 Object Lambda, consultez la liste de codes d'erreur S3 Object Lambda dans la Référence d'API Amazon Simple Storage Service API.

Pour plus d'informations sur le débogage de fonction Lambda générale, consultez Surveillance et dépannage des applications Lambda dans le Guide du développeur AWS Lambda .

Pour plus d'informations sur les erreurs Simple Storage Service (Amazon S3) standard, consultez Réponses d'erreur dans la Référence d'API Amazon Simple Storage Service.

Vous pouvez activer les métriques de demande dans Amazon CloudWatch pour vos points d'accès Object Lambda. Ces métriques vous aident à surveiller les performances opérationnelles de votre point d'accès. Vous pouvez activer les métriques de demande pendant ou après la création de votre point d'accès Object Lambda. Pour plus d'informations, consultez Métriques de demande Lambda d'un objet S3 dans CloudWatch.

Pour obtenir une journalisation plus détaillée des demandes adressées à vos points d'accès Object Lambda, vous pouvez activer les événements de données AWS CloudTrail . Pour plus d'informations, veuillez consulter Consignation d'événements de données pour les journaux d'activité dans le Guide de l'utilisateur AWS CloudTrail .

Pour obtenir des didacticiels S3 Object Lambda, consultez :

- Didacticiel : Transformation de données pour votre application avec S3 Object Lambda
- Didacticiel : Détecter et expurger des DPI avec S3 Object Lambda et Amazon Comprehend

- Tutoriel : Utilisation de S3 Object Lambda pour filigraner dynamiquement des images au fur et à mesure de leur récupération

Pour plus d'informations sur les points d'accès standard, consultez Gestion de l'accès aux jeux de données avec des points d'accès .

Pour plus d'informations sur l'utilisation des compartiments, consultez Présentation des compartiments à usage général. Pour en savoir plus sur l'utilisation des objets, consultez Présentation des objets Amazon S3.

Exécution d'opérations groupées sur des objets avec les opérations par lot

Vous pouvez utiliser les opérations par lot S3 pour effectuer des opérations par lot à grande échelle sur des objets Amazon S3. Les opérations par lot S3 peuvent effectuer une seule opération sur les listes d'objets Amazon S3 que vous spécifiez. Une seule tâche peut effectuer une opération spécifiée sur des milliards d'objets contenant des exaoctets de données. Amazon S3 suit la progression, envoie des notifications et stocke un rapport de fin d'opérations détaillé sur toutes les actions, offrant ainsi une expérience sans serveur entièrement gérée et contrôlable. Vous pouvez utiliser S3 Batch Operations via la console Amazon S3 ou AWS SDKs l'API REST Amazon S3. AWS CLI

Utilisez S3 Batch Operations pour copier des objets et définir des balises d'objets ou des listes de contrôle d'accès (ACLs). Vous pouvez également lancer des restaurations d'objets à partir de S3 Glacier Flexible Retrieval ou invoquer une fonction AWS Lambda pour effectuer des actions personnalisées à l'aide de vos objets. Vous pouvez effectuer ces opérations sur une liste d'objets personnalisée ou utiliser un rapport Amazon S3 Inventory pour faciliter la génération de listes d'objets. Les opérations par lots Amazon S3 utilisent les mêmes opérations d'API Amazon S3 que celles que vous utilisez déjà avec Amazon S3.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires. Pour plus d'informations sur l'utilisation des opérations par lots avec S3 Express One Zone et les compartiments de répertoires, consultez Utilisation des opérations par lots avec les compartiments de répertoires.

Principes de base des opérations par lot S3

Vous pouvez utiliser les opérations par lot S3 pour effectuer des opérations par lot à grande échelle sur des objets Amazon S3. Les opérations par lot S3 peuvent exécuter une seule opération ou action sur des listes d'objets Amazon S3 que vous spécifiez.

Terminologie

Cette section utilise les termes manifeste, tâches, opérations et sous-tâches, dont la définition est la suivante :

Manifeste

Un manifeste est un objet Amazon S3 qui contient les clés d'objet sur lesquelles Amazon S3 doit agir. Si vous souhaitez créer une tâche d'opérations par lot, vous devez fournir un manifeste. Votre manifeste généré par l'utilisateur doit contenir le nom du compartiment, la clé d'objet et, facultativement, la version de chaque objet. Si vous fournissez un manifeste généré par l'utilisateur, il doit se présenter sous la forme d'un rapport d'inventaire Amazon S3 ou d'un fichier CSV.

Vous pouvez aussi indiquer à Amazon S3 de générer automatiquement un manifeste en fonction des critères de filtre d'objet que vous spécifiez lors de la création de la tâche. Cette option est disponible pour les tâches de réplication par lots S3 que vous créez dans la console Amazon S3, ou pour tout type de tâche que vous créez à l'aide de l'API REST AWS Command Line Interface (AWS CLI) ou Amazon S3. AWS SDKs

Tâche

Une tâche est l'unité de travail de base des opérations par lot S3. Une tâche contient toutes les informations nécessaires à l'exécution de l'opération spécifiée pour les objets répertoriés dans le manifeste. Une fois que vous avez fourni ces informations et que vous demandez le lancement de la tâche, celle-ci effectue l'opération pour chaque objet présent dans le manifeste.

Opération

L'opération est le type d'action d'API, telle que la copie d'objets, que vous souhaitez faire exécuter par la tâche d'opérations par lot. Chaque tâche effectue un seul type d'opération sur tous les objets spécifiés dans le manifeste.

Sous-tâche

Une sous-tâche est l'unité d'exécution d'une tâche. Une tâche représente un appel unique à une opération Amazon S3 ou AWS Lambda API pour effectuer l'opération de la tâche sur un seul objet. Pendant toute la durée de vie d'une tâche, les opérations par lot S3 créent une seule tâche pour chaque objet spécifié dans le manifeste.

Fonctionnement d'une tâche d'opérations par lot S3

Une tâche est l'unité de travail de base des opérations par lot S3. Une tâche contient toutes les informations nécessaires à l'exécution de l'opération spécifiée pour une liste d'objets. Pour créer une tâche, vous fournissez aux opérations par lot S3 une liste d'objets et vous spécifiez l'action à exécuter sur ces objets.

Pour plus d'informations sur les opérations prises en charge par les opérations par lot S3, consultez Opérations prises en charge par les opérations par lot S3.

Une tâche par lot exécute une opération spécifiée sur chaque objet inclus dans son manifeste. Un manifeste répertorie les objets que vous souhaitez traiter par le biais d'une tâche par lot et il est stocké sous forme d'objet dans un compartiment. Vous pouvez utiliser un rapport Catalogage et analyse de vos données avec l'inventaire S3 au format comma-separated values (CSV) comme manifeste, ce qui facilite la création de grandes listes d'objets situés dans un compartiment. Vous pouvez également spécifier un manifeste dans un format CSV simple qui vous permet d'effectuer des opérations par lots sur une liste personnalisée d'objets stockés dans un compartiment unique.

Une fois que vous avez créé une tâche, Amazon S3 traite la liste d'objets du manifeste et exécute l'opération spécifiée sur chaque objet. Pendant qu'une tâche est en cours, vous pouvez surveiller sa progression par programme ou via la console Amazon S3. Vous pouvez également configurer une tâche pour générer un rapport de fin lorsque celle-ci se termine. Le rapport de fin décrit les résultats de chaque sous-tâche. Pour plus d'informations sur la surveillance des tâches, consultez Gestion des tâches d'opérations par lot S3.

Des coûts sont associés aux opérations par lots S3. Vous êtes facturé pour la création de tâches Batch Operations, y compris les tâches annulées avant leur fin. Pour plus d'informations, consultez Tarification Amazon S3.

S3Par défaut, les tâches Batch Operations peuvent traiter jusqu'à 4 milliards d'objets pour toutes les opérations. Plus précisément, les tâches Copy, Object Tagging, Object Lock, invocation d'une AWS Lambda fonction et Batch Replication peuvent prendre en charge jusqu'à 20 milliards d'objets.

Il existe une limite de 6 tâches de réplication par lots actives par AWS compte. Pour commencer à créer une tâche Batch Operations, consultez Création d'une tâche Batch Operations S3.

Tutoriel des opérations par lots S3

Le didacticiel suivant présente end-to-end des procédures complètes pour certaines tâches d'opérations par lots.

- Didacticiel : transcodage par lot de vidéos avec les opérations par lot S3

Octroi d'autorisations pour les opérations par lots

Avant de créer et d'exécuter des tâches d'opérations par lot S3, vous devez accorder les autorisations requises. Pour créer une tâche d'opérations par lot Amazon S3, l'autorisation de l'utilisateur `s3:CreateJob` est requise. La même entité qui crée la tâche doit également être `iam:PassRole` autorisée à transmettre le rôle AWS Identity and Access Management (IAM) spécifié pour la tâche à Batch Operations.

Pour plus d'informations générales sur la spécification des ressources IAM, consultez Éléments de stratégie JSON IAM : Ressource dans le Guide de l'utilisateur IAM. Les sections suivantes fournissent des informations sur la création d'un rôle IAM et l'attachement de stratégies.

Rubriques

- Création d'un rôle IAM pour les opérations par lot S3
- Attachement des stratégies d'autorisations

Création d'un rôle IAM pour les opérations par lot S3

Amazon S3 doit avoir l'autorisation d'effectuer des tâches d'opérations par lot S3 en votre nom. Vous accordez ces autorisations via un rôle AWS Identity and Access Management (IAM). Cette section fournit des exemples de stratégies d'approbation et d'autorisation que vous utilisez lors de la création d'un rôle IAM. Pour plus d'informations, consultez Rôles IAM dans le Guide de l'utilisateur IAM. Pour obtenir des exemples, consultez Contrôle des autorisations pour les opérations par lot à l'aide de balises de tâche et Copie d'objets à l'aide d'opérations par lot S3.

Dans vos politiques IAM, vous pouvez également utiliser des clés de condition pour filtrer les autorisations d'accès pour les tâches d'opérations par lot S3. Pour obtenir plus d'informations ainsi

que la liste complète des clés de condition spécifiques à Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Stratégie d'approbation

Vous attachez la stratégie d'approbation suivante au rôle IAM afin de permettre au principal de service de la fonctionnalité d'opérations par lot S3 d'endosser le rôle.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Attachement des stratégies d'autorisations

En fonction du type d'opérations, vous pouvez attacher l'une des stratégies suivantes.

Avant de configurer les autorisations, veuillez noter ce qui suit :

- Indépendamment de l'opération, Amazon S3 a besoin d'autorisations pour lire l'objet manifeste depuis votre compartiment S3 et, éventuellement, écrire un rapport dans votre compartiment. Dès lors, toutes les stratégies d'autorisations suivantes incluent ces autorisations.
- Pour les manifestes de rapport Amazon S3 Inventory, S3 Batch Operations nécessite l'autorisation de lire l'objet manifest.json et tous les fichiers de données CSV associés.
- Des autorisations spécifiques à la version comme `s3:GetObjectVersion` sont requises uniquement quand vous spécifiez l'ID de version des objets.

- Si vous exécutez S3 Batch Operations sur des objets chiffrés, le rôle IAM doit également avoir accès aux AWS KMS clés utilisées pour les chiffrer.
- Si vous soumettez un manifeste de rapport d'inventaire chiffré avec AWS KMS, votre politique IAM doit inclure les autorisations relatives à l'objet manifest.json `"kms:Decrypt"` et `"kms:GenerateDataKey"` à tous les fichiers de données CSV associés.
- Si la tâche Batch Operations génère un manifeste dans un bucket dans lequel les listes de contrôle d'accès (ACLs) sont activées et qui se trouve dans un autre compartiment Compte AWS, vous devez accorder l'`s3:PutObjectAcl`autorisation dans la politique IAM du rôle IAM configuré pour la tâche par lots. Si vous n'incluez pas cette autorisation, le traitement par lot échoue avec l'erreur `Error occurred when preparing manifest: Failed to write manifest`.

Copie d'objets : PutObject

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectTagging"
            ],
            "Effect": "Allow",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        },
        {
            "Action": [
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:ListBucket"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket",
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
            ]
        },
```

```
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Remplacement des balises d'objet : PutObjectTagging

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
```

```
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

Suppression du balisage d'un objet : DeleteObjectTagging

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "s3:DeleteObjectTagging",
              "s3:DeleteObjectVersionTagging"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
```

```
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Remplacement de la liste de contrôle d'accès : PutObjectAcl

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
```

```
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}
```

Restauration des objets : RestoreObject

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
          "s3:RestoreObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
```

```
  ]
}
```

Application de la rétention du verrouillage d'objet : PutObjectRetention

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention",
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
```

```
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Applications de la conservation légale du verrouillage d'objet : PutObjectLegalHold

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            ]
        },
        {
            "Effect": "Allow",
            "Action": "s3:PutObjectLegalHold",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
```

```
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
        }
    ]
}
```

Réplication d'objets existants : InitiateReplication avec un manifeste généré par S3

Optez pour cette politique si vous utilisez et stockez un manifeste généré par S3. Pour plus d'informations sur l'utilisation des opérations par lot pour répliquer des objets existants, consultez Réplication d'objets existants via la réplication par lot.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
```

```
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

Réplication d'objets existants : InitiateReplication avec un manifeste utilisateur

Utilisez cette politique si vous utilisez un manifeste fourni par l'utilisateur. Pour plus d'informations sur l'utilisation des opérations par lot pour répliquer des objets existants, consultez Réplication d'objets existants via la réplication par lot.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
```

```
            "Action":[
               "s3:GetObject",
               "s3:GetObjectVersion"
            ],
            "Effect":"Allow",
            "Resource":[
               "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
         },
         {
            "Effect":"Allow",
            "Action":[
               "s3:PutObject"
            ],
            "Resource":[
               "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
            ]
         }
      ]
}
```

Création d'une tâche d'opérations par lot S3

Les opérations par lots Amazon S3 vous permettent d'effectuer des opérations par lots à grande échelle sur une liste d'objets Amazon S3 spécifiques. Cette section décrit les informations dont vous avez besoin pour créer une tâche d'opérations par lot S3 ainsi que les résultats d'une demande `CreateJob`. Il fournit également des instructions pour créer une tâche Batch Operations à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Lorsque vous créez une tâche d'opérations par lot S3, vous pouvez demander un rapport de fin de tâche pour toutes les tâches ou uniquement pour les tâches qui ont échoué. Tant qu'au moins une tâche a été invoquée avec succès, les opérations par lots S3 génèrent un rapport pour les tâches qui ont été achevées, qui ont échoué ou qui ont été annulées. Pour plus d'informations, consultez Exemples : Rapports de fin de tâche d'opérations par lot S3.

Rubriques

- Éléments d'une demande de tâche d'opération par lot
- Spécification d'un manifeste

Éléments d'une demande de tâche d'opération par lot

Pour créer une tâche d'opérations par lot S3, vous devez fournir les informations suivantes :

Opération

Spécifiez l'opération que la tâche d'opérations par lot S3 doit exécuter sur les objets du manifeste. Chaque type d'opération accepte des paramètres spécifiques à cette opération. Avec Batch Operations, vous pouvez effectuer une opération en bloc, avec les mêmes résultats que si vous aviez effectué cette opération one-by-one sur chaque objet.

Manifeste

Le manifeste est la liste de tous les objets sur lesquels vous voulez que les opérations par lots S3 exécutent l'opération spécifiée. Vous pouvez utiliser les méthodes suivantes pour spécifier un manifeste pour une tâche d'opérations par lot :

- Créez manuellement votre propre liste d'objets personnalisée au format CSV.
- Choisissez un rapport Catalogage et analyse de vos données avec l'inventaire S3 existant au format CSV.
- Indiquez aux opérations par lots de générer automatiquement un manifeste en fonction des critères de filtre d'objet que vous spécifiez lors de la création de votre tâche. Cette option est disponible pour les tâches de réplication par lots que vous créez dans la console Amazon S3, ou pour tout type de tâche que vous créez à l'aide de l'API REST AWS CLI AWS SDKs, ou Amazon S3.

> **Note**
>
> - Quelle que soit la manière dont vous spécifiez votre manifeste, la liste elle-même doit être stockée dans un compartiment à usage général. Les opérations par lots ne peuvent pas importer de manifestes existants à partir de compartiments de répertoires, ni enregistrer les manifestes générés dans ces compartiments. Toutefois, les objets décrits dans le manifeste peuvent être stockés dans des compartiments de répertoires. Pour plus d'informations, consultez Compartiments de répertoires.
> - Si les objets de votre manifeste se trouvent dans un compartiment versionné, la spécification de la version IDs des objets indique à Batch Operations d'effectuer l'opération sur une version spécifique. Si aucune version IDs n'est spécifiée, Batch Operations exécute l'opération sur la dernière version des objets. Si votre manifeste

comprend un champ d'identification de version, vous devez fournir un identifiant de version pour tous les objets du manifeste.

Pour plus d'informations, consultez Spécification d'un manifeste.

Priority

Utilisez les priorités pour indiquer la priorité relative de cette tâche par rapport aux autres s'exécutant dans votre compte. Un nombre plus élevé indique une priorité plus élevée.

Les priorités n'ont de sens que par rapport aux priorités établies pour d'autres tâches dans le même compte et la même Région. Ainsi, vous pouvez choisir le système de numérotation qui vous convient. Par exemple, vous souhaiterez peut-être attribuer à toutes les tâches Restore (`RestoreObject`) une priorité de 1, à toutes les tâches Copy (`CopyObject`) une priorité de 2 et à toutes les tâches Replace des listes de contrôle d'accès (ACLs**`PutObjectAcl`**) () une priorité de 3.

Les opérations par lots S3 traitent les tâches en fonction de leur numéro de priorité, mais un ordre strict n'est pas garanti. Par conséquent, n'utilisez pas les priorités de tâche pour vous assurer qu'une tâche commence ou finit avant une autre. Si vous devez garantir un ordre strict, attendez qu'une tâche se termine avant de démarrer la suivante.

RoleArn

Spécifiez un rôle AWS Identity and Access Management (IAM) pour exécuter la tâche. Le rôle IAM que vous utilisez doit avoir les autorisations suffisantes pour exécuter l'opération spécifiée dans la tâche. Par exemple, pour exécuter une tâche `CopyObject`, le rôle IAM doit avoir l'autorisation `s3:GetObject` pour le compartiment source et l'autorisation `s3:PutObject` pour le compartiment de destination. Le rôle a également besoin des autorisations pour lire le manifeste et écrire le rapport de fin de tâche.

Pour plus d'informations sur les rôles IAM, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations Amazon S3, consultez Actions de politique pour Amazon S3.

> **Note**
>
> Les tâches d'opérations par lots qui effectuent des actions sur des compartiments de répertoires nécessitent des autorisations spécifiques. Pour plus d'informations, consultez AWS Identity and Access Management (IAM) pour S3 Express One Zone.

Rapport

Indiquez si vous souhaitez que la fonctionnalité d'opérations par lot S3 génère un rapport d'achèvement. Si vous demandez un rapport de fin de tâche, vous devez également fournir les paramètres du rapport dans cet élément. Les informations nécessaires sont les suivantes :

- Le compartiment dans lequel vous souhaitez stocker le rapport

  > **Note**
  >
  > Le rapport doit être stocké dans un compartiment à usage général. Les opérations par lots ne peuvent pas enregistrer les rapports dans des compartiments de répertoires. Pour plus d'informations, consultez Compartiments de répertoires.

- Le format du rapport
- Si vous souhaitez que le rapport comprenne les détails de toutes les tâches ou uniquement de celles ayant échoué
- Une chaîne de préfixe facultative

> **Note**
>
> Les rapports de fin de tâche sont toujours chiffrés avec un chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

Les balises (facultatif)

Vous pouvez étiqueter et contrôler l'accès à vos tâches d'opérations par lot S3 en ajoutant des étiquettes. Vous pouvez utiliser des balises pour identifier qui est responsable d'une tâche d'opérations par lots ou pour contrôler comment les utilisateurs interagissent avec les tâches d'opérations par lot. La présence d'étiquettes de tâche peut octroyer ou limiter la capacité d'un utilisateur à annuler une tâche, activer une tâche dans l'état de confirmation ou

modifier le niveau de priorité d'une tâche. Par exemple, vous pouvez accorder à un utilisateur l'autorisation d'invoquer l'opération `CreateJob`, à condition que la tâche soit créée avec la balise `"Department=Finance"`.

Vous pouvez créer des tâches avec des étiquettes qui leur sont attachées et ajouter des étiquettes aux travaux après les avoir créés.

Pour plus d'informations, consultez the section called "Utilisation d'étiquettes".

Description (facultative)

Pour suivre et surveiller votre tâche, vous pouvez également fournir une description de 256 caractères maximum. Amazon S3 inclut cette description chaque fois qu'il renvoie des informations sur une tâche ou affiche les détails de la tâche sur la console Amazon S3. Cela vous permet de trier et filtrer facilement les tâches en fonction des descriptions que vous avez allouées. Comme les descriptions n'ont pas à être uniques, vous pouvez utiliser les descriptions comme catégories (par exemple, « Tâches hebdomadaires de copie des journaux ») pour vous aider à suivre les groupes de tâches similaires.

Spécification d'un manifeste

Un manifeste est un objet Amazon S3 qui contient les clés d'objet sur lesquelles Amazon S3 doit agir. Vous pouvez fournir un manifeste de différentes manières :

- Créez manuellement un nouveau fichier manifeste.
- Utilisez un manifeste existant.
- Indiquez aux opérations par lots de générer automatiquement un manifeste en fonction des critères de filtre d'objet que vous spécifiez lors de la création de votre tâche. Cette option est disponible pour les tâches de réplication par lots que vous créez dans la console Amazon S3, ou pour tout type de tâche que vous créez à l'aide de l'API REST AWS CLI AWS SDKs, ou Amazon S3.

> **Note**
>
> - Les opérations par lot Amazon S3 ne prennent pas en charge la génération de manifestes entre régions.
> - Quelle que soit la manière dont vous spécifiez votre manifeste, la liste elle-même doit être stockée dans un compartiment à usage général. Les opérations par lots ne peuvent pas

importer de manifestes existants à partir de compartiments de répertoires, ni enregistrer les manifestes générés dans ces compartiments. Toutefois, les objets décrits dans le manifeste peuvent être stockés dans des compartiments de répertoires. Pour plus d'informations, consultez Compartiments de répertoires.

Création d'un fichier manifeste

Pour créer un fichier manifeste manuellement, vous devez spécifier la clé de l'objet manifeste ETag (balise d'entité) et l'ID de version facultatif dans une liste au format CSV. Les contenus du manifeste doivent être codés au format URL.

Par défaut, Amazon S3 utilise automatiquement le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) pour chiffrer un manifeste chargé dans un compartiment Amazon S3. Les manifestes qui utilisent un chiffrement côté serveur avec des clés fournies par le client (SSE-C) ne sont pas pris en charge. Les manifestes qui utilisent le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) ne sont pris en charge que lorsque vous utilisez des rapports d'inventaire au format CSV. L'utilisation d'un manifeste créé manuellement avec n' AWS KMS est pas prise en charge.

Votre manifeste doit contenir le nom du compartiment, la clé d'objet et, facultativement, la version de chaque objet. Les autres champs du manifeste ne sont pas utilisés lors des opérations par lot S3.

> **Note**
>
> Si les objets de votre manifeste se trouvent dans un compartiment versionné, la spécification de la version IDs des objets indique à Batch Operations d'effectuer l'opération sur une version spécifique. Si aucune version IDs n'est spécifiée, Batch Operations exécute l'opération sur la dernière version des objets. Si votre manifeste comprend un champ d'identification de version, vous devez fournir un identifiant de version pour tous les objets du manifeste.

Voici un exemple de manifeste au format CSV sans version IDs.

```
amzn-s3-demo-bucket1,objectkey1
amzn-s3-demo-bucket1,objectkey2
amzn-s3-demo-bucket1,objectkey3
amzn-s3-demo-bucket1,photos/jpgs/objectkey4
```

```
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5
amzn-s3-demo-bucket1,object%20key%20with%20spaces
```

Voici un exemple de manifeste au format CSV qui inclut la version IDs.

```
amzn-s3-demo-bucket1,objectkey1,PZ9ibn9D5lP6p298B7S9_ceqx1n5EJ0p
amzn-s3-demo-bucket1,objectkey2,YY_ouuAJByNW1LRBfFMfxMge7XQWxMBF
amzn-s3-demo-bucket1,objectkey3,jbo9_jhdPEyB4RrmOxWS0kU0EoNrU_oI
amzn-s3-demo-bucket1,photos/jpgs/objectkey4,6EqlikJJxLTsHsnbZbSRffn24_eh5Ny4
amzn-s3-demo-bucket1,photos/jpgs/newjersey/objectkey5,imHf3FAiRsvBW_EHB8GOu.NHunHO1gVs
amzn-s3-demo-bucket1,object%20key%20with%20spaces,9HkPvDaZY5MVbMhn6TMn1YTb5ArQAo3w
```

Spécification d'un fichier manifeste existant

Vous pouvez spécifier un fichier manifeste pour une demande de création de tâche dans l'un des deux formats suivants :

- Rapport d'inventaire Amazon S3 : il doit s'agir d'un rapport d'inventaire Amazon S3 au format CSV. Vous devez spécifier le fichier `manifest.json` associé au rapport d'inventaire. Pour plus d'informations sur les rapports d'inventaire, consultez Catalogage et analyse de vos données avec l'inventaire S3. Si le rapport d'inventaire inclut la version IDs, S3 Batch Operations fonctionne sur les versions d'objets spécifiques.

  > **Note**
  >
  > - Les opérations par lots S3 prennent en charge des rapports d'inventaire CSV chiffrés avec SSE-KMS.
  > - Si vous soumettez un manifeste de rapport d'inventaire chiffré avec SSE-KMS, votre politique IAM doit inclure les autorisations `"kms:Decrypt"` et `"kms:GenerateDataKey"` pour l'objet `manifest.json` et tous les fichiers de données CSV associés.

- Fichier CSV : chaque ligne du fichier doit inclure le nom du compartiment, la clé d'objet et, éventuellement, la version de l'objet. Les clés d'objets doivent être encodées en URL, comme montré dans les exemples suivants. Le manifeste doit inclure la version IDs pour tous les objets ou omettre la version IDs pour tous les objets. Pour plus d'informations sur le format de manifeste CSV, consultez JobManifestSpec dans la Référence d'API Amazon Simple Storage Service.

> **Note**
>
> Les opérations par lots S3 ne prennent pas en charge les fichiers manifestes CSV chiffrés avec SSE-KMS.

> **Important**
>
> Lorsque vous utilisez un manifeste créé manuellement et un compartiment versionné, nous vous recommandons de spécifier la version IDs des objets. Lorsque vous créez une tâche, les opérations par lot S3 analysent l'intégralité du manifeste avant d'exécuter la tâche. Cependant, cela ne crée pas d'instantané de l'état de ce compartiment.
> Les manifestes pouvant contenir des milliards d'objets, l'exécution des tâches peut prendre beaucoup de temps, ce qui peut avoir une incidence sur la version d'un objet sur laquelle la tâche agit. Supposons que vous remplaciez un objet par une nouvelle version pendant qu'une tâche s'exécute et que vous n'avez pas spécifié d'ID de version pour cet objet. Dans ce cas, Amazon S3 effectue l'opération sur la dernière version de l'objet, et non pas sur la version qui existait lorsque vous avez créé la tâche. Le seul moyen d'éviter ce comportement est de spécifier IDs la version des objets répertoriés dans le manifeste.

Génération automatique d'un manifeste

Vous pouvez indiquer à Amazon S3 de générer automatiquement un manifeste en fonction des critères de filtre d'objet que vous spécifiez lors de la création de la tâche. Cette option est disponible pour les tâches de réplication par lots que vous créez dans la console Amazon S3, ou pour tout type de tâche que vous créez à l'aide de l'API REST AWS CLI AWS SDKs, ou Amazon S3. Pour en savoir plus sur la réplication par lot, consultez Réplication d'objets existants via la réplication par lot.

Pour générer automatiquement un manifeste, vous devez spécifier les éléments suivants dans le cadre de votre demande de création de tâche :

- Des informations sur le compartiment qui contient vos objets sources, y compris le propriétaire du compartiment et l'Amazon Resource Name (ARN)
- Des informations relatives à la sortie du manifeste, notamment un indicateur permettant de créer un fichier manifeste, le propriétaire du compartiment de sortie, l'ARN, le préfixe, le format de fichier et le type de chiffrement

- Des critères facultatifs pour filtrer les objets par date de création, nom de clé, taille et classe de stockage Dans le cas des tâches de réplication, vous pouvez également utiliser les balises pour filtrer les objets.

Critères de filtre d'objet

Pour filtrer la liste des objets à inclure dans un manifeste généré automatiquement, vous pouvez spécifier les critères suivants. Pour plus d'informations, consultez JobManifestGeneratorFilter dans la Référence d'API Amazon S3.

CreatedAfter

Si ce critère est fourni, le manifeste généré inclut uniquement les objets du compartiment source créés après cet instant.

CreatedBefore

Si ce critère est fourni, le manifeste généré inclut uniquement les objets du compartiment source créés avant cet instant.

EligibleForReplication

Si ce critère est fourni, le manifeste généré inclut les objets uniquement s'ils sont éligibles à la réplication conformément à la configuration de réplication du compartiment source.

KeyNameConstraint

S'il est fourni, le manifeste généré inclut uniquement les objets du compartiment source dont les clés d'objet correspondent aux contraintes de chaîne spécifiées pour MatchAnySubstringMatchAnyPrefix, et MatchAnySuffix.

MatchAnySubstring— S'il est fourni, le manifeste généré inclut des objets si la chaîne spécifiée apparaît n'importe où dans la chaîne clé de l'objet.

MatchAnyPrefix— S'il est fourni, le manifeste généré inclut des objets si la chaîne spécifiée apparaît au début de la chaîne clé de l'objet.

MatchAnySuffix— S'il est fourni, le manifeste généré inclut des objets si la chaîne spécifiée apparaît à la fin de la chaîne clé de l'objet.

MatchAnyStorageClass

Si ce critère est fourni, le manifeste généré inclut uniquement les objets du compartiment source stockés avec la classe de stockage spécifiée.

ObjectReplicationStatuses

Si ce critère est fourni, le manifeste généré inclut uniquement les objets du compartiment source présentant l'un des statuts de réplication spécifiés.

ObjectSizeGreaterThanBytes

Si ce critère est fourni, le manifeste généré inclut uniquement les objets du compartiment source dont la taille de fichier est supérieure au nombre d'octets spécifié.

ObjectSizeLessThanBytes

Si ce critère est fourni, le manifeste généré inclut uniquement les objets du compartiment source dont la taille de fichier est inférieure au nombre d'octets spécifié.

> **Note**
>
> Vous ne pouvez pas cloner la plupart des tâches qui ont généré automatiquement des manifestes. Les tâches de réplication par lot peuvent être clonées, sauf lorsqu'elles utilisent les critères de filtre de manifeste `KeyNameConstraint`, `MatchAnyStorageClass`, `ObjectSizeGreaterThanBytes` ou `ObjectSizeLessThanBytes`.

La syntaxe permettant de spécifier les critères du manifeste varie en fonction de la méthode que vous utilisez pour créer votre tâche. Pour obtenir des exemples, consultez Création d'une tâche.

Création d'une tâche

Vous pouvez créer des tâches S3 Batch Operations à l'aide de la console Amazon S3 ou de l'API REST Amazon S3. AWS CLI AWS SDKs

Pour plus d'informations sur la création d'une demande de tâche, consultez Éléments d'une demande de tâche d'opération par lot.

Prérequis

Avant de créer une tâche d'opérations par lot, vérifiez que vous avez configuré les autorisations pertinentes. Pour plus d'informations, consultez Octroi d'autorisations pour les opérations par lots.

Utilisation de la console S3

Pour créer une tâche par lot

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, sélectionnez le nom de la Région AWS actuellement affichée. Choisissez la région dans laquelle vous souhaitez créer la tâche.

   > **Note**
   >
   > Pour les opérations de copie, vous devez créer la tâche dans la même région que le compartiment de destination. Pour toutes les autres opérations, vous devez créer la tâche dans la même région que les objets figurant dans le manifeste.

3. Choisissez Opérations par lot dans le volet de navigation de gauche de la console Amazon S3.
4. Choisissez Créer une tâche.
5. Affichez la Région AWS dans laquelle vous souhaitez créer votre tâche.
6. Sous Format du manifeste, choisissez le type d'objet manifeste à utiliser.

   - Si vous choisissez S3 inventory report (Rapport sur l'inventaire S3), entrez le chemin de l'objet manifest.json généré par Amazon S3 dans le cadre du rapport d'inventaire au format CSV et éventuellement l'ID de version de l'objet manifeste si vous souhaitez utiliser une version autre que la version la plus récente.
   - Si vous choisissez CSV, entrez le chemin vers un objet manifeste au format CSV. L'objet manifeste doit respecter le format décrit dans la console. Vous pouvez éventuellement inclure l'ID de version de l'objet manifeste si vous souhaitez utiliser une version autre que la plus récente.

   > **Note**
   >
   > La console Amazon S3 prend en charge la génération automatique de manifeste uniquement pour les tâches de réplication par lot. Pour tous les autres types de tâches, si vous souhaitez qu'Amazon S3 génère automatiquement un manifeste en fonction des critères de filtre que vous spécifiez, vous devez configurer votre tâche à l'aide de l'API REST AWS CLI AWS SDKs, ou Amazon S3.

7. Choisissez Suivant.
8. Sous Operation (Opération), choisissez l'opération que vous souhaitez effectuer sur tous les objets répertoriés dans le manifeste. Remplissez les informations relatives à l'opération choisie, puis sélectionnez Suivant.
9. Remplissez les informations relatives à l'option Configure additional options (Configurer les options supplémentaires), puis sélectionnez Suivant.
10. Sous Vérification, vérifiez les paramètres. Si vous devez apporter des modifications, choisissez Précédent. Sinon, choisissez Créer une tâche.

À l'aide du AWS CLI

Pour créer votre tâche Batch Operations avec le AWS CLI, choisissez l'un des exemples suivants, selon que vous spécifiez un manifeste existant ou que vous générez un manifeste automatiquement.

Specify manifest

L'exemple suivant montre comment utiliser le AWS CLI pour créer une `S3PutObjectTagging` tâche S3 Batch Operations qui agit sur des objets répertoriés dans un fichier manifeste existant.

Pour créer une tâche **`S3PutObjectTagging`** d'opérations par lots en spécifiant un manifeste

1. Utilisez les commandes suivantes pour créer un rôle AWS Identity and Access Management (IAM), puis créez une politique IAM pour attribuer les autorisations appropriées. Le rôle et la politique suivants accordent à Amazon S3 l'autorisation d'ajouter des balises d'objet, dont vous aurez besoin lors de la création de la tâche dans une étape ultérieure.

   a. Utilisez l'exemple de commande suivant pour créer un rôle IAM qui sera utilisé par les opérations par lot. Pour utiliser cet exemple de commande, remplacez *`S3BatchJobRole`* par le nom que vous souhaitez donner à ce rôle.

```
aws iam create-role \
 --role-name S3BatchJobRole \
 --assume-role-policy-document '{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
```

```
        },
        "Action":"sts:AssumeRole"
      }
   ]
}'
```

Prenez note de l'Amazon Resource Name (ARN) du rôle. Vous aurez besoin de l'ARN lors de la création d'une tâche.

b. Utilisez l'exemple de commande suivant pour créer une politique IAM avec les autorisations nécessaires et l'attacher au rôle IAM que vous avez créé à l'étape précédente. Pour plus d'informations sur les autorisations nécessaires, consultez Octroi d'autorisations pour les opérations par lots.

> **Note**
>
> Les tâches d'opérations par lots qui effectuent des actions sur des compartiments de répertoires nécessitent des autorisations spécifiques. Pour plus d'informations, consultez AWS Identity and Access Management (IAM) pour S3 Express One Zone.

Pour utiliser cet exemple de commande, remplacez les *user input placeholders* comme suit :

- Remplacez *S3BatchJobRole* par le nom de votre rôle IAM. Assurez-vous que ce nom correspond au nom que vous avez utilisé précédemment.
- Remplacez *PutObjectTaggingBatchJobPolicy* par le nom que vous souhaitez donner à la politique IAM.
- Remplacez *amzn-s3-demo-destination-bucket* par le nom du compartiment qui contient les objets auxquels vous souhaitez appliquer des balises.
- Remplacez *amzn-s3-demo-manifest-bucket* par le nom du compartiment qui contient le manifeste.
- Remplacez *amzn-s3-demo-completion-report-bucket* par le nom du compartiment dans lequel vous voulez livrer le rapport d'achèvement.

```
aws iam put-role-policy \
```

```
  --role-name S3BatchJobRole \
  --policy-name PutObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObjectTagging",
        "s3:PutObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:GetBucketLocation"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
      ]
    }
  ]
}'
```

2. Utilisez l'exemple de commande suivant pour créer une tâche `S3PutObjectTagging`.

   Le fichier `manifest.csv` fournit une liste des valeurs de compartiment et de clé d'objet. Cette tâche applique les balises spécifiées aux objets identifiés dans le manifeste. `ETagIl`

s'agit ETag de l'`manifest.csv`objet, que vous pouvez obtenir depuis la console Amazon S3. Cette demande spécifie le paramètre `no-confirmation-required`, afin que vous puissiez exécuter la tâche sans avoir à la confirmer avec la commande `update-job-status`. Pour plus d'informations, consultez create-job dans la Référence des commandes de l'AWS CLI .

Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations. Remplacez *`IAM-role`* par l'ARN du rôle IAM que vous avez créé auparavant.

```
aws s3control create-job \
    --region us-west-2 \
    --account-id acct-id \
    --operation '{"S3PutObjectTagging": { "TagSet": [{"Key":"keyOne",
 "Value":"ValueOne"}] }}' \
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket/manifest.csv","ETag":"60e460c9d1046e73f7dde5043ac3ae85"}}' \
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
completion-report-bucket","Prefix":"final-reports",
 "Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
    --priority 42 \
    --role-arn IAM-role \
    --client-request-token $(uuidgen) \
    --description "job description" \
    --no-confirmation-required
```

En réponse, Amazon S3 renvoie un ID de tâche (par exemple, `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`). Vous aurez besoin de l'ID de la tâche pour identifier, surveiller et modifier la tâche.

Generate manifest

L'exemple suivant montre comment créer une tâche d'opérations par lots S3 `S3DeleteObjectTagging` qui génère automatiquement un manifeste en fonction de vos critères de filtre d'objet. Ces critères incluent la date de création, le nom de la clé, la taille, la classe de stockage et les balises.

Pour créer une tâche **`S3DeleteObjectTagging`** d'opérations par lots en générant un manifeste

1. Utilisez les commandes suivantes pour créer un rôle AWS Identity and Access Management (IAM), puis créez une politique IAM pour attribuer des autorisations. Le rôle et la politique suivants accordent à Amazon S3 l'autorisation de supprimer des balises d'objet, dont vous aurez besoin lors de la création de la tâche dans une étape ultérieure.

   a. Utilisez l'exemple de commande suivant pour créer un rôle IAM qui sera utilisé par les opérations par lot. Pour utiliser cet exemple de commande, remplacez *`S3BatchJobRole`* par le nom que vous souhaitez donner à ce rôle.

```
aws iam create-role \
 --role-name S3BatchJobRole \
 --assume-role-policy-document '{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}'
```

   Prenez note de l'Amazon Resource Name (ARN) du rôle. Vous aurez besoin de l'ARN lors de la création d'une tâche.

   b. Utilisez l'exemple de commande suivant pour créer une politique IAM avec les autorisations nécessaires et l'attacher au rôle IAM que vous avez créé à l'étape précédente. Pour plus d'informations sur les autorisations nécessaires, consultez Octroi d'autorisations pour les opérations par lots.

> **Note**
>
> Les tâches d'opérations par lots qui effectuent des actions sur des compartiments de répertoires nécessitent des autorisations spécifiques. Pour

plus d'informations, consultez AWS Identity and Access Management (IAM) pour S3 Express One Zone.

Pour utiliser cet exemple de commande, remplacez les *user input placeholders* comme suit :

- Remplacez *S3BatchJobRole* par le nom de votre rôle IAM. Assurez-vous que ce nom correspond au nom que vous avez utilisé précédemment.
- Remplacez *DeleteObjectTaggingBatchJobPolicy* par le nom que vous souhaitez donner à la politique IAM.
- Remplacez *amzn-s3-demo-destination-bucket* par le nom du compartiment qui contient les objets auxquels vous souhaitez appliquer des balises.
- Remplacez *amzn-s3-demo-manifest-bucket* par le nom du compartiment dans lequel vous voulez enregistrer le manifeste.
- Remplacez *amzn-s3-demo-completion-report-bucket* par le nom du compartiment dans lequel vous voulez livrer le rapport d'achèvement.

```
aws iam put-role-policy \
  --role-name S3BatchJobRole \
  --policy-name DeleteObjectTaggingBatchJobPolicy \
  --policy-document '{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutInventoryConfiguration"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "s3:PutObject",
        "s3:ListBucket"
      ],
      "Resource":[
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
    }
  ]
}'
```

2. Utilisez l'exemple de commande suivant pour créer la tâche `S3DeleteObjectTagging`.

   Dans cet exemple, les valeurs de la section `--report` spécifient le compartiment, le préfixe, le format et la portée du rapport de tâche qui sera généré. La section `--manifest-generator` fournit des informations sur le compartiment source qui contient les objets sur lesquels la tâche agira, des informations sur la liste de sortie du manifeste qui sera générée pour la tâche et les critères de filtre permettant de réduire l'étendue des objets à inclure dans le manifeste en fonction de la date de création, de contraintes de nom, de la taille et de la classe de stockage. La commande spécifie également la priorité de la tâche, le rôle IAM et la Région AWS.

   Pour plus d'informations, consultez create-job dans la Référence des commandes de l'AWS CLI .

Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations. Remplacez *IAM-role* par l'ARN du rôle IAM que vous avez créé auparavant.

```
aws s3control create-job \
    --account-id 012345678901 \
    --operation '{
        "S3DeleteObjectTagging": {}
    }' \
    --report '{
        "Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
        "Prefix":"reports",
        "Format":"Report_CSV_20180820",
        "Enabled":true,
        "ReportScope":"AllTasks"
    }' \
    --manifest-generator '{
        "S3JobManifestGenerator": {
          "ExpectedBucketOwner": "012345678901",
          "SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket",
          "EnableManifestOutput": true,
          "ManifestOutputLocation": {
            "ExpectedManifestBucketOwner": "012345678901",
            "Bucket": "arn:aws:s3:::amzn-s3-demo-manifest-bucket",
            "ManifestPrefix": "prefix",
            "ManifestFormat": "S3InventoryReport_CSV_20211130"
          },
          "Filter": {
            "CreatedAfter": "2023-09-01",
            "CreatedBefore": "2023-10-01",
            "KeyNameConstraint": {
              "MatchAnyPrefix": [
                "prefix"
              ],
              "MatchAnySuffix": [
                "suffix"
              ]
            },
            "ObjectSizeGreaterThanBytes": 100,
            "ObjectSizeLessThanBytes": 200,
            "MatchAnyStorageClass": [
              "STANDARD",
```

```
            "STANDARD_IA"
          ]
        }
      }
    }' \
    --priority 2 \
    --role-arn IAM-role \
    --region us-east-1
```

En réponse, Amazon S3 renvoie un ID de tâche (par exemple, `00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c`). Vous aurez besoin de cet ID de tâche pour identifier, surveiller ou modifier la tâche.

À l'aide du AWS SDK pour Java

Pour créer votre tâche Batch Operations avec le AWS SDK pour Java, choisissez l'un des exemples suivants, selon que vous spécifiez un manifeste existant ou que vous générez un manifeste automatiquement.

Specify manifest

L'exemple suivant montre comment créer une tâche d'opérations par lots S3 `S3PutObjectTagging` qui agit sur les objets répertoriés dans un fichier manifeste existant. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

Example

```
package aws.example.s3control;



import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.*;

import java.util.UUID;
import java.util.ArrayList;

import static com.amazonaws.regions.Regions.US_WEST_2;
```

```
public class CreateJob {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String iamRoleArn = "IAM Role ARN";
        String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
        String uuid = UUID.randomUUID().toString();

        ArrayList tagSet = new ArrayList<S3Tag>();
        tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));


        try {
            JobOperation jobOperation = new JobOperation()
                    .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
                            .withTagSet(tagSet)
                    );

            JobManifest manifest = new JobManifest()
                    .withSpec(new JobManifestSpec()
                            .withFormat("S3BatchOperations_CSV_20180820")
                            .withFields(new String[]{
                                    "Bucket", "Key"
                            }))
                    .withLocation(new JobManifestLocation()
                            .withObjectArn("arn:aws:s3:::my_manifests/manifest.csv")
                            .withETag("60e460c9d1046e73f7dde5043ac3ae85"));
            JobReport jobReport = new JobReport()
                    .withBucket(reportBucketName)
                    .withPrefix("reports")
                    .withFormat("Report_CSV_20180820")
                    .withEnabled(true)
                    .withReportScope("AllTasks");

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.createJob(new CreateJobRequest()
                    .withAccountId(accountId)
                    .withOperation(jobOperation)
                    .withManifest(manifest)
```

```
                    .withReport(jobReport)
                    .withPriority(42)
                    .withRoleArn(iamRoleArn)
                    .withClientRequestToken(uuid)
                    .withDescription("job description")
                    .withConfirmationRequired(false)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Generate manifest

L'exemple suivant montre comment créer une tâche d'opérations par lots S3 `s3PutObjectCopy` qui génère automatiquement un manifeste en fonction de vos critères de filtre d'objet, dont notamment la date de création, le nom de clé et la taille. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

Example

```
        package aws.example.s3control;

    import com.amazonaws.AmazonServiceException;
    import com.amazonaws.SdkClientException;
    import com.amazonaws.auth.profile.ProfileCredentialsProvider;
    import com.amazonaws.services.s3control.AWSS3Control;
    import com.amazonaws.services.s3control.AWSS3ControlClient;
    import com.amazonaws.services.s3control.model.CreateJobRequest;
    import com.amazonaws.services.s3control.model.CreateJobResult;
    import com.amazonaws.services.s3control.model.JobManifestGenerator;
    import com.amazonaws.services.s3control.model.JobManifestGeneratorFilter;
    import com.amazonaws.services.s3control.model.JobOperation;
    import com.amazonaws.services.s3control.model.JobReport;
    import com.amazonaws.services.s3control.model.KeyNameConstraint;
```

```
    import com.amazonaws.services.s3control.model.S3JobManifestGenerator;
    import com.amazonaws.services.s3control.model.S3ManifestOutputLocation;
    import com.amazonaws.services.s3control.model.S3SetObjectTaggingOperation;
    import com.amazonaws.services.s3control.model.S3Tag;

    import java.time.Instant;
    import java.util.Date;
    import java.util.UUID;
    import java.util.ArrayList;

    import static com.amazonaws.regions.Regions.US_WEST_2;

    public class test {
        public static void main(String[] args) {
            String accountId = "012345678901";
            String iamRoleArn = "arn:aws:iam::012345678901:role/ROLE";
            String sourceBucketName = "arn:aws:s3:::amzn-s3-demo-source-bucket";
            String reportBucketName = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
            String manifestOutputBucketName = "arn:aws:s3:::amzn-s3-demo-manifest-
bucket";
            String uuid = UUID.randomUUID().toString();
            long minimumObjectSize = 100L;

            ArrayList<S3Tag> tagSet = new ArrayList<>();
            tagSet.add(new S3Tag().withKey("keyOne").withValue("ValueOne"));

            ArrayList<String> prefixes = new ArrayList<>();
            prefixes.add("s3KeyStartsWith");

            try {
                JobOperation jobOperation = new JobOperation()
                        .withS3PutObjectTagging(new S3SetObjectTaggingOperation()
                                .withTagSet(tagSet)
                        );
                S3ManifestOutputLocation manifestOutputLocation = new
 S3ManifestOutputLocation()
                        .withBucket(manifestOutputBucketName)
                        .withManifestPrefix("manifests")
                        .withExpectedManifestBucketOwner(accountId)
                        .withManifestFormat("S3InventoryReport_CSV_20211130");

                JobManifestGeneratorFilter jobManifestGeneratorFilter = new
 JobManifestGeneratorFilter()
```

```
                        .withEligibleForReplication(true)
                        .withKeyNameConstraint(
                                new KeyNameConstraint()
                                        .withMatchAnyPrefix(prefixes))
                        .withCreatedBefore(Date.from(Instant.now()))
                        .withObjectSizeGreaterThanBytes(minimumObjectSize);

                S3JobManifestGenerator s3JobManifestGenerator = new
S3JobManifestGenerator()
                        .withEnableManifestOutput(true)
                        .withManifestOutputLocation(manifestOutputLocation)
                        .withFilter(jobManifestGeneratorFilter)
                        .withSourceBucket(sourceBucketName);

                JobManifestGenerator jobManifestGenerator = new
JobManifestGenerator()
                        .withS3JobManifestGenerator(s3JobManifestGenerator);

                JobReport jobReport = new JobReport()
                        .withBucket(reportBucketName)
                        .withPrefix("reports")
                        .withFormat("Report_CSV_20180820")
                        .withEnabled(true)
                        .withReportScope("AllTasks");

                AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                        .withCredentials(new ProfileCredentialsProvider())
                        .withRegion(US_WEST_2)
                        .build();

                CreateJobResult createJobResult = s3ControlClient.createJob(new
CreateJobRequest()
                        .withAccountId(accountId)
                        .withOperation(jobOperation)
                        .withManifestGenerator(jobManifestGenerator)
                        .withReport(jobReport)
                        .withPriority(42)
                        .withRoleArn(iamRoleArn)
                        .withClientRequestToken(uuid)
                        .withDescription("job description")
                        .withConfirmationRequired(true)
                );

                System.out.println("Created job " + createJobResult.getJobId());
```

```
            } catch (AmazonServiceException e) {
                // The call was transmitted successfully, but Amazon S3 couldn't
process
                // it and returned an error response.
                e.printStackTrace();
            } catch (SdkClientException e) {
                // Amazon S3 couldn't be contacted for a response, or the client
                // couldn't parse the response from Amazon S3.
                e.printStackTrace();
            }
        }
    }
```

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour créer une tâche d'opérations par lot. Pour plus d'informations, consultez CreateJob dans la Référence d'API Amazon Simple Storage Service.

Réponses à la tâche

Si la demande `CreateJob` aboutit, Amazon S3 renvoie un ID de tâche. L'ID de tâche est un identifiant unique généré automatiquement par Amazon S3 afin que vous puissiez identifier votre tâche d'opérations par lot et surveiller son statut.

Lorsque vous créez une tâche via l'API AWS CLI AWS SDKs, ou REST, vous pouvez configurer S3 Batch Operations pour commencer à traiter la tâche automatiquement. La tâche s'exécute dès qu'elle est prête, au lieu d'attendre que des tâches de plus haute priorité soient traitées en premier.

Lorsque vous créez une tâche via la console Amazon S3, vous devez vérifier les détails de la tâche et confirmer que vous voulez l'exécuter avant que les opérations par lots commencent à la traiter. Si une tâche conserve l'état Suspendu pendant plus de 30 jours, cette tâche échouera.

Opérations prises en charge par les opérations par lot S3

Vous pouvez utiliser les opérations par lot S3 pour effectuer des opérations par lot à grande échelle sur des objets Amazon S3. Les opérations par lot S3 peuvent effectuer une seule opération sur les listes d'objets Amazon S3 que vous spécifiez. Une seule tâche peut effectuer une opération spécifiée sur des milliards d'objets contenant des exaoctets de données. Amazon S3 suit la progression, envoie des notifications et stocke un rapport de fin d'opérations détaillé sur toutes les actions, offrant

ainsi une expérience sans serveur entièrement gérée et contrôlable. Vous pouvez utiliser S3 Batch Operations via la console Amazon S3 ou AWS SDKs l'API REST Amazon S3. AWS CLI

Les opérations par lots S3 prennent en charge les opérations suivantes :

Copie d'objets

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. L'opération par lot Copier copie chaque objet spécifié dans le manifeste. Vous pouvez copier des objets dans un compartiment de la même région Région AWS ou dans un compartiment d'une autre région. Les opérations par lot S3 supportent la plupart des options disponibles via Amazon S3 pour copier des objets. Ces options comprennent la définition des métadonnées d'objet, la spécification d'autorisations et la modification de la classe de stockage d'un objet.

Vous pouvez utiliser l'opération Copier pour copier des objets non chiffrés et les réécrire dans le même compartiment en tant qu'objets chiffrés. Pour plus d'informations, consultez Chiffrement d'objets avec des opérations par lot Amazon S3.

Lorsque vous copiez des objets, vous pouvez modifier l'algorithme de contrôle utilisé pour calculer le total de contrôle de l'objet. Si les objets n'ont pas de total de contrôle calculé, vous pouvez également en ajouter un en spécifiant l'algorithme de total de contrôle à utiliser pour Amazon S3. Pour de plus amples informations, veuillez consulter Vérification de l'intégrité des objets dans Amazon S3.

Pour plus d'informations sur la copie d'objets dans Amazon S3, ainsi que sur les paramètres obligatoires et facultatifs, consultez Copie, déplacement et changement de nom des objets dans ce guide et CopyObject dans la Référence d'API Amazon Simple Storage Service.

Restrictions et limitations

Lorsque vous utilisez l'opération Copier des opérations par lot, les restrictions et limites suivantes s'appliquent :

- Tous les objets sources doivent se trouver dans un même compartiment.
- Tous les objets de destination doivent se trouver dans un même compartiment.
- Vous devez disposer d'autorisations de lecture pour le compartiment source et d'autorisations d'écriture pour le compartiment de destination.
- La taille des objets à copier peut aller jusqu'à 5 Go.

- Si vous essayez de copier des objets depuis les classes S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive dans la classe de stockage S3 Standard, vous devez d'abord restaurer ces objets. Pour de plus amples informations, veuillez consulter Restauration d'un objet archivé.
- Vous devez créer les tâches Copier des opérations par lot dans la région de destination, à savoir la région dans laquelle vous prévoyez de copier les objets.
- Toutes les `CopyObject` options sont prises en charge, à l'exception des vérifications conditionnelles sur les balises d'entité (ETags) et du chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C).
- Si le compartiment de destination n'est associé à aucune version, vous écraserez tous les objets dont le nom de clé est le même.
- Les objets ne sont pas nécessairement copiés dans le même ordre que celui dans lequel ils apparaissent dans le manifeste. Pour les compartiments pour lesquels la gestion des versions est activée, si la préservation de l'ordre des versions actuelles ou anciennes est importante, copiez d'abord toutes les anciennes versions. Ensuite, une fois la première tâche terminée, copiez les versions actuelles dans une tâche ultérieure.
- La copie d'objets vers la classe de stockage à redondance réduite (RRS) n'est pas prise en charge.
- Une seule tâche Batch Operations Copy peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

Copie d'objets à l'aide d'opérations par lot S3

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. Vous pouvez utiliser la fonctionnalité d'opérations par lot S3 pour créer une tâche de copie (`CopyObject`) dans le but de copier des objets dans un même compte ou dans un autre compte de destination.

Les sections suivantes montrent comment stocker et utiliser un manifeste qui se trouve dans un compte différent. Le premier exemple présente comment utiliser l'inventaire Amazon S3 pour remettre le rapport d'inventaire au compte de destination afin de l'utiliser lors de la création de la tâche. Le deuxième exemple montre comment utiliser un manifeste de valeurs séparées par des virgules (CSV) dans le compte source ou de destination. Le troisième exemple montre comment utiliser l'opération Copier pour activer les clés de compartiment S3 pour des objets existants qui ont été chiffrés à l'aide du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS).

Exemples d'opérations de copie

- Utilisation d'un rapport d'inventaire pour copier des objets Comptes AWS
- Utilisation d'un manifeste CSV pour copier des objets Comptes AWS
- Utilisation des opérations par lot pour activer les clés de compartiment S3 pour SSE-KMS

Utilisation d'un rapport d'inventaire pour copier des objets Comptes AWS

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. Vous pouvez utiliser la fonctionnalité d'opérations par lot S3 pour créer une tâche de copie (`CopyObject`) dans le but de copier des objets dans un même compte ou dans un autre compte de destination.

Vous pouvez utiliser un inventaire Amazon S3 pour créer un rapport d'inventaire, et utiliser ce rapport pour créer une liste, ou un manifeste, des objets à copier avec les opérations par lot S3. Pour de plus amples informations sur l'utilisation d'un manifeste CSV dans le compte source ou de destination, consultez the section called "Utilisation d'un manifeste CSV pour copier des objets Comptes AWS".

L'inventaire Amazon S3 génère des inventaires des objets dans un compartiment. La liste générée est publiée dans un fichier de sortie. Le compartiment qui est inventorié est appelé le compartiment source et le compartiment où le fichier de rapport d'inventaire est stocké est appelé le compartiment de destination.

Le rapport d'inventaire Amazon S3 peut être configuré pour être envoyé à un autre Compte AWS. Cela permet à la fonctionnalité d'opérations par lot S3 de lire le rapport d'inventaire lorsque la tâche a été créée dans le compte de destination.

Pour de plus amples informations sur les compartiments sources et de destination de l'inventaire Amazon S3, consultez Compartiments source et de destination.

Le moyen le plus simple de configurer un inventaire est d'utiliser la console Amazon S3, mais vous pouvez également utiliser l'API REST Amazon S3, AWS Command Line Interface (AWS CLI) ou AWS SDKs.

La procédure de console suivante contient les étapes de haut niveau permettant de configurer des autorisations pour une tâche d'opérations par lot S3. Dans cette procédure, vous copiez des objets d'un compte source vers un compte de destination, avec le rapport d'inventaire stocké dans le compte de destination.

Pour configurer Amazon S3 Inventory pour des compartiments source et de destination détenus par des comptes différents

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Définissez (ou créez) un compartiment de manifeste de destination dans lequel stocker le rapport d'inventaire. Dans cette procédure, le compte de destination est le compte qui possède à la fois le compartiment de manifeste de destination et le compartiment où les objets sont copiés.
4. Configurez un rapport d'inventaire pour un compartiment source. Pour plus d'informations sur l'utilisation de la console pour configurer un inventaire ou sur le chiffrement d'un fichier de liste d'inventaire, consultez Configuration de l'inventaire Amazon S3.

   Lorsque vous configurez un rapport d'inventaire, vous spécifiez le compartiment de destination dans lequel vous souhaitez stocker la liste. Le rapport d'inventaire pour le compartiment source est publié dans le compartiment de destination. Dans cette procédure, le compte source est le compte qui possède le compartiment source.

   Choisissez CSV comme format de sortie.

   Lorsque vous saisissez des informations pour le compartiment de destination, choisissez Compartiments d'un autre compte. Ensuite, saisissez le nom du compartiment de manifeste de destination. Éventuellement, vous pouvez saisir l'ID du compte de destination.

   Une fois que la configuration d'inventaire a été enregistrée, la console affiche un message similaire au message suivant :

   Amazon S3 n'a pas pu créer une stratégie sur le compartiment de destination. Demandez au propriétaire du compartiment de destination d'ajouter la politique de compartiment suivante pour permettre à Amazon S3 d'ajouter des données dans ce compartiment.

   Ensuite, la console affiche une politique de compartiment que vous pouvez utiliser pour le compartiment de destination.
5. Copiez la politique de compartiment de destination qui apparaît sur la console.
6. Dans le compte de destination, ajoutez la politique de compartiment copiée dans le compartiment de manifeste de destination où le rapport d'inventaire est stocké.

7. Créez un rôle dans le compte de destination basé sur la stratégie d'approbation de la fonctionnalité d'opérations par lot S3. Pour plus d'informations sur la politique d'approbation, consultez Stratégie d'approbation.

   Pour plus d'informations sur la création d'un rôle, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

   Saisissez un nom pour le rôle (l'exemple de rôle suivant utilise le nom *BatchOperationsDestinationRoleCOPY*). Choisissez le service S3, puis choisissez le cas d'utilisation Opérations par lot S3, lequel appliquera la politique d'approbation au rôle.

   Ensuite, choisissez Create policy (Créer une stratégie) pour attacher la stratégie suivante au rôle. Pour utiliser cette politique, remplacez *user input placeholders* par vos propres informations.

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
      ]
```

```
    }
  ]
}
```

Le rôle utilise la stratégie pour autoriser `batchoperations.s3.amazonaws.com` à lire le manifeste dans le compartiment de destination. Il accorde également des autorisations aux GET objets, aux listes de contrôle d'accès (ACLs), aux balises et aux versions du compartiment d'objets source. Il accorde également des autorisations aux PUT objets ACLs, aux balises et aux versions dans le compartiment d'objets de destination.

8. Dans le compte source, créez une politique de compartiment pour le compartiment source qui accorde au rôle que vous avez créé à l'étape précédente des autorisations sur les GET objets ACLs, les balises et les versions du compartiment source. Cette étape permet à la fonctionnalité d'opérations par lot S3 de récupérer des objets du compartiment source au moyen du rôle approuvé.

   Vous trouverez, ci-après, un exemple de politique de compartiment pour le compte source. Pour utiliser cette politique, remplacez *`user input placeholders`* par vos propres informations.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowBatchOperationsSourceObjectCOPY",
            "Effect": "Allow",
            "Principal": {
                "AWS":
 "arn:aws:iam::111122223333:role/BatchOperationsDestinationRoleCOPY"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetObjectAcl",
                "s3:GetObjectTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
```

```
        }
    ]
}
```

9. Une fois le rapport d'inventaire disponible, créez une tâche Copier (`CopyObject`) d'opérations par lot S3 dans le compte de destination, en choisissant le rapport d'inventaire dans le compartiment du manifeste de destination. Vous aurez besoin de l'ARN du rôle IAM que vous avez créé dans le compte de destination.

   Pour obtenir des informations générales sur la création d'une tâche, consultez Création d'une tâche d'opérations par lot S3.

   Pour plus d'informations sur la création d'une tâche à l'aide de la console, consultez Création d'une tâche d'opérations par lot S3.

Utilisation d'un manifeste CSV pour copier des objets Comptes AWS

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. Vous pouvez utiliser la fonctionnalité d'opérations par lot S3 pour créer une tâche de copie (`CopyObject`) dans le but de copier des objets dans un même compte ou dans un autre compte de destination.

Vous pouvez utiliser un manifeste CSV stocké dans le compte source pour copier des objets dans des Comptes AWS avec les opérations par lot S3. Pour utiliser un rapport d'inventaire S3 en tant que manifeste, consultez the section called "Utilisation d'un rapport d'inventaire pour copier des objets Comptes AWS".

Pour obtenir un exemple du format CSV pour les fichiers manifestes, consultez the section called "Création d'un fichier manifeste".

La procédure suivante montre comment configurer des autorisations lors de l'utilisation d'une tâche d'opérations par lot S3 pour copier des objets d'un compte source vers un compte de destination avec un fichier manifeste CSV stocké dans le compte source.

Pour utiliser un manifeste CSV pour copier des objets Comptes AWS

1. Créez un rôle AWS Identity and Access Management (IAM) dans le compte de destination basé sur la politique de confiance de S3 Batch Operations. Dans cette procédure, le compte de destination est le compte dans lequel les objets sont copiés.

Pour de plus amples informations sur la stratégie d'approbation, consultez Stratégie d'approbation.

Pour plus d'informations sur la création d'un rôle, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

Si vous créez le rôle au moyen de la console, saisissez un nom pour ce rôle (l'exemple de rôle suivant utilise le nom *BatchOperationsDestinationRoleCOPY*). Choisissez le service S3, puis choisissez le cas d'utilisation Opérations par lot S3, lequel appliquera la politique d'approbation au rôle.

Ensuite, choisissez Create policy (Créer une stratégie) pour attacher la stratégie suivante au rôle. Pour utiliser cette politique, remplacez *user input placeholders* par vos propres informations.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsDestinationObjectCOPY",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectVersionAcl",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectTagging",
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
```

```
      ]
    }
  ]
}
```

Au moyen de la stratégie, le rôle octroie à `batchoperations.s3.amazonaws.com` l'autorisation de lire le manifeste dans le compartiment manifeste source. Il accorde des autorisations aux `GET` objets, aux listes de contrôle d'accès (ACLs), aux balises et aux versions du compartiment d'objets source. Il accorde également des autorisations aux `PUT` objets ACLs, aux balises et aux versions dans le compartiment d'objets de destination.

2. Dans le compte source, créez une politique pour le compartiment, qui contient le manifeste afin d'octroyer au rôle créé à l'étape précédente l'autorisation d'obtenir (`GET`) des objets et des versions dans le compartiment manifeste source.

   Cette étape permet à la fonctionnalité d'opérations par lot S3 de lire le manifeste au moyen du rôle approuvé. Appliquez la politique de compartiment au compartiment qui contient le manifeste.

   Vous trouverez, ci-après, un exemple de politique de compartiment à appliquer au compartiment manifeste source. Pour utiliser cette politique, remplacez *`user input placeholders`* par vos propres informations.

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceManfiestRead",
      "Effect": "Allow",
      "Principal": {
        "AWS": [

 "arn:aws:iam::DestinationAccountNumber:user/ConsoleUserCreatingJob",

 "arn:aws:iam::DestinationAccountNumber:role/
BatchOperationsDestinationRoleCOPY"
        ]
      },
      "Action": [
```

```
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
    }
  ]
}
```

Cette stratégie octroie également à un utilisateur de la console qui est en train de créer une tâche dans le compte de destination les mêmes autorisations dans le compartiment manifeste source au moyen de la même politique de compartiment.

3. Dans le compte source, créez une politique de compartiment pour le compartiment source qui accorde au rôle dans lequel vous avez créé des autorisations sur les GET objets ACLs, les balises et les versions du compartiment d'objets source. La fonctionnalité d'opérations par lot S3 peut ensuite récupérer des objets du compartiment source via le rôle approuvé.

   Vous trouverez, ci-après, un exemple de politique de compartiment pour le compartiment qui contient les objets source. Pour utiliser cette politique, remplacez *user input placeholders* par vos propres informations.

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowBatchOperationsSourceObjectCOPY",
      "Effect": "Allow",
      "Principal": {
        "AWS":
 "arn:aws:iam::DestinationAccountNumber:role/
BatchOperationsDestinationRoleCOPY"
      },
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
```

```
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
    }
  ]
}
```

4. Créez une tâche d'opérations par lot S3 dans le compte de destination. Vous avez besoin de l'ARN (Amazon Resource Name) pour le rôle que vous avez créé dans le compte de destination. Pour de plus amples informations sur la création d'une tâche, consultez Création d'une tâche d'opérations par lot S3.

Utilisation des opérations par lot pour activer les clés de compartiment S3 pour SSE-KMS

Les clés de compartiment S3 réduisent le coût du chiffrement côté serveur avec AWS Key Management Service (AWS KMS) (SSE-KMS) en diminuant le trafic de requêtes d'Amazon S3 vers. AWS KMS Pour plus d'informations, consultez Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3 et Configuration de votre compartiment de sorte qu'il utilise une clé de compartiment S3 avec SSE-KMS pour de nouveaux objets. Lorsque vous effectuez une `CopyObject` opération à l'aide de l'API REST AWS SDKs, ou AWS CLI, vous pouvez activer ou désactiver une clé de compartiment S3 au niveau de l'objet en ajoutant l'en-tête de `x-amz-server-side-encryption-bucket-key-enabled` demande avec une `false` valeur `true` ou.

Lorsque vous configurez une clé de compartiment S3 pour un objet à l'aide d'une opération `CopyObject`, Amazon S3 met à jour uniquement les paramètres de cet objet. Les paramètres de clé de compartiment S3 pour le compartiment de destination ne changent pas. Si vous soumettez une demande `CopyObject` pour un objet chiffré par AWS KMS dans un compartiment avec les clés de compartiment S3 activées, votre opération au niveau de l'objet utilisera automatiquement cette option à moins que vous ne désactiviez les clés dans l'en-tête de la demande. Si vous ne spécifiez pas de clé de compartiment S3 pour votre objet, Amazon S3 applique les paramètres de clé de compartiment S3 du compartiment de destination à l'objet.

Pour chiffrer vos objets Amazon S3 existants, vous pouvez utiliser des opérations par lot S3. Vous pouvez utiliser l'opération de copie des opérations par lot pour copier des objets non chiffrés et les réécrire dans le même compartiment en tant qu'objets chiffrés. Pour plus d'informations, consultez la section Chiffrement d'objets avec Amazon S3 Batch Operations sur le blog AWS de stockage.

Dans l'exemple suivant, vous utilisez la tâche Copier des opérations par lot pour activer les clés de compartiment S3 sur des objets existants. Pour de plus amples informations, veuillez consulter the section called "Configuration d'une clé de compartiment S3 pour un objet".

Rubriques

- Considérations pour l'utilisation d'opérations pat lot S3 pour chiffrer des objets avec des clés de compartiment S3
- Prérequis
- Étape 1 : obtenir votre liste d'objets à l'aide d'Amazon S3 Inventory
- Étape 2 : filtrer votre liste d'objets avec S3 Select
- Étape 3 : configurer et exécuter votre tâche d'opérations par lot S3

Considérations pour l'utilisation d'opérations pat lot S3 pour chiffrer des objets avec des clés de compartiment S3

Lorsque vous utilisez les opérations par lot S3 pour chiffrer des objets avec les clés de compartiment S3 activées, tenez compte des points suivants :

- Vous serez facturé pour les tâches, objets et demandes d'opérations par lot S3 en plus des frais associés à ce que les opérations par lot S3 accomplissent en votre nom, dont les transferts de données, les demandes, ainsi que d'autres frais. Pour de plus amples informations, veuillez consulter Tarification Amazon S3.
- Si vous utilisez un compartiment avec gestion des versions, chaque tâche d'opérations par lot S3 effectuée crée de nouvelles versions chiffrées de vos objets. Elle conserve également les versions précédentes sans clé de compartiment S3 configurée. Pour supprimer les anciennes versions, configurez une stratégie d'expiration du cycle de vie S3 pour les versions non actuelles, comme décrit dans Éléments de la configuration du cycle de vie.
- L'opération de copie crée de nouveaux objets avec de nouvelles dates de création, ce qui peut affecter des actions du cycle de vie telles que l'archivage. Si vous copiez tous les objets dans votre compartiment, toutes les nouvelles copies ont des dates de création identiques ou similaires. Pour mieux identifier ces objets et créer différentes règles de cycle de vie pour différents sous-ensembles de données, envisagez d'utiliser des étiquettes d'objet.

Prérequis

Avant de configurer les objets de sorte qu'ils utilisent une clé de compartiment S3, consultez Modifications à prendre en compte avant d'activer une clé de compartiment S3.

Pour utiliser cet exemple, vous devez disposer d'un compartiment S3 Compte AWS et d'au moins un compartiment S3 pour contenir vos fichiers de travail et vos résultats chiffrés. Il se peut également

que vous trouviez des informations utiles dans une grande partie de la documentation existante sur les opérations par lot S3, dont les rubriques suivantes :

- Principes de base des opérations par lot S3
- Création d'une tâche d'opérations par lot S3
- Opérations prises en charge par les opérations par lot S3
- Gestion des tâches d'opérations par lot S3

Étape 1 : obtenir votre liste d'objets à l'aide d'Amazon S3 Inventory

Pour commencer, identifiez le compartiment S3 contenant les objets à chiffrer, et obtenez la liste de son contenu. Un rapport d'inventaire Amazon S3 est le moyen le plus pratique et le plus abordable de le faire. Le rapport fournit la liste des objets dans un compartiment ainsi que les métadonnées associées. Dans cette étape, le compartiment source fait référence au compartiment inventorié, et le compartiment de destination au compartiment dans lequel vous stockez le fichier de rapport d'inventaire. Pour de plus amples informations sur les compartiments sources et de destination de l'inventaire Amazon S3, consultez Catalogage et analyse de vos données avec l'inventaire S3.

La manière la plus simple de configurer un inventaire consiste à utiliser la AWS Management Console. Mais vous pouvez également utiliser l'API REST, AWS Command Line Interface (AWS CLI) ou AWS SDKs. Avant de suivre ces étapes, assurez-vous de vous connecter à la console et d'ouvrir la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/. Si vous rencontrez des erreurs de refus d'autorisation, ajoutez une politique de compartiment à votre compartiment de destination. Pour de plus amples informations, veuillez consulter Accorder des autorisations pour l'inventaire S3 et les analyses S3..

Pour obtenir une liste d'objets à l'aide d'un inventaire S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments et sélectionnez un compartiment contenant des objets à chiffrer.
3. Sous l'onglet Management (Gestion), accédez à la section Inventory configurations (Configurations d'inventaire), puis choisissez Create inventory configuration (Créer une configuration d'inventaire).
4. Donnez un nom à votre nouvel inventaire, entrez le nom du compartiment S3 de destination, et créez éventuellement un préfixe de destination pour Amazon S3 afin d'affecter des objets dans ce compartiment.

5. Pour Output format (Format de sortie), choisissez CSV.
6. (Facultatif) Dans la section Champs supplémentaires - facultatif, choisissez Chiffrement et les autres champs de rapport qui vous intéressent. Définissez la fréquence de livraison des rapports sur Daily (Quotidienne) afin que le premier rapport soit livré à votre compartiment plus tôt.
7. Choisissez Create (Créer) pour enregistrer votre configuration.

Amazon S3 peut prendre jusqu'à 48 heures pour livrer le premier rapport. Guettez donc l'arrivée de votre premier rapport. Après avoir reçu votre premier rapport, passez à la section suivante pour filtrer le contenu de votre rapport d'inventaire S3. Si vous ne souhaitez plus recevoir de rapports d'inventaire pour ce compartiment, supprimez votre configuration d'inventaire S3. Autrement, S3 continue de livrer les rapports à une fréquence quotidienne ou hebdomadaire.

Une liste d'inventaire n'est pas une point-in-time vue unique de tous les objets. Une liste d'inventaire est un instantané évolutif des éléments d'un compartiment, qui sont finalement cohérents (par exemple, il se peut que la liste n'inclue pas certains objets récemment ajoutés ou supprimés). La combinaison de l'inventaire S3 et des opérations par lot S3 fonctionne de façon optimale lorsque vous travaillez avec des objets statiques, ou avec un ensemble d'objets que vous avez créé au moins deux jours auparavant. Pour travailler avec des données plus récentes, utilisez l'opération d'API ListObjectsV2 (compartiment `GET`) pour établir manuellement votre liste d'objets. Si nécessaire, répétez le processus pendant quelques jours ou jusqu'à ce que le rapport d'inventaire affiche le statut souhaité pour tous les objets.

Étape 2 : filtrer votre liste d'objets avec S3 Select

Après avoir reçu votre rapport d'inventaire S3, vous pouvez filtrer son contenu pour répertorier uniquement les objets qui ne sont pas chiffrés avec des clés de compartiment S3 activées. Si vous voulez que tous les objets de votre compartiment soient chiffrés avec des clés de compartiment S3, vous pouvez ignorer cette étape. Toutefois, le filtrage du rapport d'inventaire S3 à ce stade vous permet d'économiser du temps et de l'argent en lien avec le re-chiffrement des objets que vous avez chiffrés précédemment avec les clés de compartiment S3 activées.

Bien que les étapes suivantes montrent comment filtrer le rapport à l'aide d'Amazon S3 Select, vous pouvez également utiliser Amazon Athena. Pour décider de l'outil à utiliser, consultez le fichier `manifest.json` de votre rapport d'inventaire S3. Ce fichier répertorie le nombre de fichiers de données associés à ce rapport. Si ce nombre est conséquent, utilisez le service Amazon Athena, car il s'exécute sur plusieurs objets S3, tandis que S3 Select opère sur un objet à la fois. Pour plus d'informations sur l'utilisation conjointe d'Amazon S3 et Athena, consultez Interrogation d'un

inventaire Amazon S3 avec Amazon Athena « Utilisation d'Athena » dans le billet de blog sur le AWS stockage Encrypting objects with Amazon S3 Batch Operations.

Pour filtrer votre rapport d'inventaire S3 avec S3 Select

1. Ouvrez le fichier `manifest.json` à partir de votre rapport d'inventaire et consultez la section `fileSchema` du fichier JSON. Celle-ci informe la requête que vous exécutez sur les données.

   Le JSON suivant est un exemple de fichier `manifest.json` pour un inventaire au format CSV dans un compartiment pour lequel la gestion des versions est activée. L'aspect de votre manifeste peut varier selon la façon dont vous avez configuré votre rapport d'inventaire.

```
  {
    "sourceBucket": "batchoperationsdemo",
    "destinationBucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
    "version": "2021-05-22",
    "creationTimestamp": "1558656000000",
    "fileFormat": "CSV",
    "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
 BucketKeyStatus",
    "files": [
      {
        "key": "demoinv/batchoperationsdemo/DemoInventory/data/009a40e4-
f053-4c16-8c75-6100f8892202.csv.gz",
        "size": 72691,
        "MD5checksum": "c24c831717a099f0ebe4a9d1c5d3935c"
      }
    ]
  }
```

   Si la gestion des versions n'est pas activée sur le compartiment, ou si vous choisissez d'exécuter le rapport pour les dernières versions, le `fileSchema` est `Bucket`, `Key` et `BucketKeyStatus`.

   Si la gestion des versions est activée, selon la façon dont vous avez configuré le rapport d'inventaire, le `fileSchema` peut inclure les éléments suivants : `Bucket`, `Key`, `VersionId`, `IsLatest`, `IsDeleteMarker` et `BucketKeyStatus`. Soyez donc attentif aux colonnes 1, 2, 3 et 6 lorsque vous exécutez votre requête.

   Les opérations par lot S3 ont besoin du compartiment, de la clé et de l'ID de version entrés pour effectuer la tâche, en plus du champ sur lequel effectuer la recherche, qui est `BucketKeyStatus`. Vous n'avez pas besoin du champ `VersionID`, mais il est utile de spécifier

`VersionID`lorsque vous opérez sur un compartiment pour lequel la gestion des versions est activée. Pour de plus amples informations, veuillez consulter Utiliser des objets dans un compartiment activé pour la gestion des versions.

2. Recherchez les fichiers de données pour le rapport d'inventaire. L'objet `manifest.json` répertorie les fichiers de données sous files.
3. Après avoir localisé et sélectionné le fichier de données dans la console S3, choisissez Actions, puis Query with S3 Select (Requête avec S3 Select).
4. Conservez la sélection des champs prédéfinis CSV,Comma, et GZIP, puis choisissez Next (Suivant).
5. Pour réviser le format de votre rapport d'inventaire avant de poursuivre, choisissez Afficher l'aperçu du fichier.
6. Saisissez les colonnes à référencer dans la zone d'expression SQL, puis sélectionnez Run SQL (Exécuter SQL). L'expression suivante renvoie les colonnes 1 à 3 pour tous les objets sans clé de compartiment S3 configurée.

   ```
   select s._1, s._2, s._3 from s3object s where s._6 = 'DISABLED'
   ```

   Voici quelques exemples de résultats.

   ```
         batchoperationsdemo,0100059%7Ethumb.jpg,lsrtIxksLu0R0ZkYPL.LhgD5caTYn6vu
         batchoperationsdemo,0100074%7Ethumb.jpg,sd2M60g6Fdazoi6D5kNARIE7KzUibmHR
         batchoperationsdemo,0100075%7Ethumb.jpg,TLYESLnl1mXD5c4BwiOIinqFrktddkoL
         batchoperationsdemo,0200147%7Ethumb.jpg,amufzfMi_fEw0Rs99rxR_HrDFlE.l3Y0
         batchoperationsdemo,0301420%7Ethumb.jpg,9qGU2SEscL.C.c_sK89trmXYIwooABSh
         batchoperationsdemo,0401524%7Ethumb.jpg,ORnEWNuB1QhHrrYAGFsZhbyvEYJ3DUor
         batchoperationsdemo,200907200065HQ
   %7Ethumb.jpg,d8LgvIVjbDR5mUVwW6pu9ahTfReyn5V4
         batchoperationsdemo,200907200076HQ
   %7Ethumb.jpg,XUT25d7.gK40u_GmnupdaZg3BVx2jN40
         batchoperationsdemo,201103190002HQ
   %7Ethumb.jpg,z.2sVRh0myqVi0BuIrngWlsRPQdb7qOS
   ```

7. Téléchargez les résultats, enregistrez-les au format CSV, et chargez-les sur Amazon S3 en tant que liste d'objets pour la tâche d'opérations par lot S3.
8. Si vous avez plusieurs fichiers manifeste, exécutez une Requête avec S3 Select sur ceux-ci. En fonction de la taille des résultats, vous pouvez combiner les listes et exécuter un seule tâche d'opérations par lot S3, ou exécuter chaque liste en tant que tâche distincte. Pour décider du

nombre de tâches à exécuter, considérez le tarif d'exécution de chaque tâche d'opérations par lot S3.

Étape 3 : configurer et exécuter votre tâche d'opérations par lot S3

À présent que vos listes CSV d'objets S3 sont filtrées, vous pouvez commencer la tâche d'opérations par lot S3 pour chiffrer les objets avec les clés de compartiment S3 activées.

Une tâche fait référence collectivement à la liste (manifeste) d'objets fournis, à l'opération effectuée et aux paramètres spécifiés. La manière la plus simple de chiffrer cet ensemble d'objets avec les clés de compartiment S3 activées consiste à utiliser l'opération Copier en spécifiant le même préfixe de destination que celui des objets répertoriés dans le manifeste. Dans un compartiment sans gestion des versions, cette opération remplace les objets existants. Dans un compartiment pour lequel la gestion des versions est activée, cette opération crée une version chiffrée plus récente des objets.

Dans le cadre de la copie des objets, spécifiez qu'Amazon S3 doit chiffrer les objets avec le chiffrement SSE-KMS. Cette tâche copie les objets. À la fin, tous vos objets présenteront donc une date de création mise à jour, quelle que soit la date à laquelle vous les avez initialement ajoutés à Amazon S3. Dans le cadre de la tâche d'opérations par lot S3, spécifiez également les autres propriétés de votre ensemble d'objets, y compris les étiquettes d'objet et la classe de stockage.

Sous-étapes

- Configurer votre politique IAM
- Configurer votre rôle IAM d'opérations par lot
- Activation des clés de compartiment S3 pour un compartiment existant
- Créer votre tâche d'opérations par lot
- Exécuter votre tâche d'opérations par lot

Configurer votre politique IAM

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, choisissez Politique, puis Créer une politique.
3. Choisissez l'onglet JSON. Choisissez Modifier la stratégie, puis ajoutez l'exemple de politique IAM qui apparaît dans le bloc de code suivant.

   Après avoir copié l'exemple de politique dans votre console IAM, effectuez les remplacements suivants :

a. Remplacez *amzn-s3-demo-source-bucket* par le nom du compartiment source à partir duquel copier les objets.

b. Remplacez *amzn-s3-demo-destination-bucket* par le nom du compartiment de destination dans lequel copier les objets.

c. Remplacez *amzn-s3-demo-manifest-bucket*/*manifest-key* par le nom de votre objet manifeste.

d. Remplacez *amzn-s3-demo-completion-report-bucket* par le nom du compartiment dans lequel vous voulez enregistrer les rapports de fin de tâche.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CopyObjectsToEncrypt",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:PutObjectTagging",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectVersionAcl",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
        "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      ]
    },
    {
      "Sid": "ReadManifest",
      "Effect": "Allow",
      "Action": [
```

```
        "s3:GetObject",
        "s3:GetObjectVersion"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest-key"
    },
    {
      "Sid": "WriteReport",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
    }
  ]
}
```

4. Choisissez Next: Tags (Suivant : Étiquettes).
5. Ajoutez les étiquettes de votre choix (facultatif), puis choisissez Next: Review (Suivant : Vérification).
6. Ajoutez un nom de stratégie et, éventuellement, une description, puis choisissez Create policy (Créer une stratégie).
7. Choisissez Review policy (Examiner une stratégie), puis Save changes (Enregistrer les modifications).
8. Une fois votre stratégie d'opérations par lot S3 prête, la console vous renvoie à l'IAM Policies (Stratégies). Filtrez le nom de stratégie, choisissez le bouton situé à gauche du nom de stratégie, choisissez Policy actions (Actions de stratégie), puis Attach (Attacher).

   Pour attacher la stratégie nouvellement créée à un rôle IAM, sélectionnez les utilisateurs, groupes ou rôles appropriés dans votre compte, puis choisissez Attach Policy (Attacher une stratégie). Cela a pour effet de vous ramener à la console IAM.

Configurer votre rôle IAM d'opérations par lot

1. Dans le volet de navigation de la console IAM, choisissez Rôles, puis Créer un rôle.
2. Sélectionnez Service AWS, S3 et Opérations par lots S3. Choisissez ensuite Next: Permissions (Suivant : Autorisations).

3. Commencer à entrer le nom de la politique IAM que vous venez de créer. Activez la case à cocher en regard du nom de stratégie quand il s'affiche, puis choisissez Next: Tags (Suivant : Étiquettes).
4. (Facultatif) Ajoutez des étiquettes ou gardez les champs de clé et de valeur vides pour cet exercice. Choisissez Next: Review (Suivant : Vérification).
5. Entrez un nom de rôle, puis acceptez la description par défaut ou ajoutez la vôtre. Sélectionnez Create role (Créer un rôle).
6. Assurez-vous que l'utilisateur qui crée la tâche dispose des autorisations décrites dans l'exemple suivant.

   Remplacez *account-id* par l'ID de votre Compte AWS , et *IAM-role-name* par le nom que vous envisagez d'appliquer au rôle IAM que vous allez créer ultérieurement à l'étape de création de tâche d'opérations par lot. Pour de plus amples informations, veuillez consulter Octroi d'autorisations pour les opérations par lots.

```
{
"Sid": "AddIamPermissions",
"Effect": "Allow",
"Action": [
"iam:GetRole",
"iam:PassRole"
],
"Resource": "arn:aws:iam::account-id:role/IAM-role-name"
}
```

Activation des clés de compartiment S3 pour un compartiment existant

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le compartiment pour lequel vous souhaitez activer une clé de compartiment S3.
3. Choisissez Propriétés.
4. Sous Default encryption (Chiffrement par défaut), choisissez Edit (Modifier).
5. Sous Type de chiffrement, vous avez le choix entre Clés gérées par Amazon S3 (SSE-S3) et CléAWS Key Management Service (SSE-KMS).
6. Si vous avez choisi AWS Key Management Service clé (SSE-KMS), sous AWS KMS key, vous pouvez spécifier la AWS KMS clé à l'aide de l'une des options suivantes.

- Pour choisir parmi la liste des clés KMS disponibles, sélectionnez Choisir parmi vos clés AWS KMS . Dans la liste des clés disponibles, choisissez une clé KMS symétrique de chiffrement dans la même région que votre compartiment. La clé AWS gérée (`aws/s3`) et les clés gérées par votre client apparaissent toutes deux dans la liste.
- Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN de votre clé KMS dans le champ qui apparaît.
- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

7. Sous Clé de compartiment, choisissez Activer, puis Enregistrer les modifications.

À présent qu'une clé de compartiment S3 est activée au niveau du compartiment, les objets chargés, modifiés ou copiés dans ce compartiment héritent de cette configuration de chiffrement par défaut. Cela inclut les objets copiés à l'aide d'opérations par lot Amazon S3.

Créer votre tâche d'opérations par lot

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Opérations par lot, puis Créer une tâche.
3. Choisissez la Région dans laquelle vous stockez vos objets, puis choisissez CSV comme type de manifeste.
4. Saisissez le chemin d'accès ou accédez au fichier manifeste CSV que vous avez créé précédemment à partir des résultats de S3 Select (ou d'Athena). Si votre manifeste contient une version IDs, cochez cette case. Choisissez Suivant.
5. Choisissez l'opération Copy (Copier), le compartiment de destination de la copie. Vous pouvez maintenir le chiffrement côté serveur désactivé. Tant que les clés de compartiment S3 sont activées pour la destination du compartiment, l'opération de copie applique ces clés à ce compartiment.
6. (Facultatif) Choisissez une classe de stockage et les autres paramètres souhaités. Les paramètres que vous spécifiez dans cette étape s'appliquent à toutes les opérations effectuées sur les objets répertoriés dans le manifeste. Choisissez Suivant.
7. Pour configurer le chiffrement côté serveur, procédez comme suit :

    a. Sous Chiffrement côté serveur, choisissez l'une des options suivantes :

        - Pour conserver les paramètres du compartiment pour le chiffrement côté serveur par défaut des objets lors de leur stockage dans Amazon S3, choisissez Ne pas spécifier

de clé de chiffrement. Tant que les clés de compartiment S3 sont activées pour la destination du compartiment, l'opération de copie applique une clé de compartiment S3 au compartiment de destination.

> **Note**
>
> Si la politique de compartiment pour la destination spécifiée exige que les objets soient chiffrés avant de les stocker dans Amazon S3, vous devez spécifier une clé de chiffrement. Sinon, la copie des objets vers la destination échouera.

- Pour chiffrer des objets avant de les stocker dans Amazon S3, choisissez Spécifier une clé de chiffrement.

b. Dans Paramètres de chiffrement, si vous choisissez Spécifier une clé de chiffrement, vous devez choisir Utiliser les paramètres du compartiment de destination pour le chiffrement par défaut ou Ignorer les paramètres du compartiment de destination pour le chiffrement par défaut.

c. Si vous choisissez Ignorer les paramètres du compartiment de destination pour le chiffrement par défaut, vous devez configurer les paramètres de chiffrement suivants.

   i. Sous Type de chiffrement, vous devez choisir Clés gérées par Amazon S3 (SSE-S3) ou CléAWS Key Management Service (SSE-KMS). SSE-S3 utilise l'un des chiffrements par bloc les plus puissants qui existent, Advanced Encryption Standard à 256 bits (AES-256) pour chiffrer chaque objet. SSE-KMS vous permet de mieux contrôler votre clé. Pour plus d'informations, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) et Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

   ii. Si vous choisissez CléAWS Key Management Service (SSE-KMS), sous AWS KMS key, vous pouvez spécifier votre AWS KMS key via l'une des options suivantes.

   - Pour choisir parmi la liste des clés KMS disponibles, choisissez Choose from your AWS KMS keys, puis choisissez une clé KMS de chiffrement symétrique dans la même région que votre bucket. La clé AWS gérée (`aws/s3`) et les clés gérées par votre client apparaissent toutes deux dans la liste.
   - Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis saisissez l'ARN de votre clé KMS dans le champ qui apparaît.
   - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

iii. Sous Clé de compartiment, choisissez Activer. L'opération de copie applique une clé de compartiment S3 au compartiment de destination.

8. Saisissez une description pour votre tâche (ou conservez la description par défaut), définissez son niveau de priorité, choisissez un type de rapport, puis spécifiez le Path to completion report destination (Chemin d'accès de la destination du rapport de fin de tâche).
9. Dans la section Permissions (Autorisations), veillez à choisir le rôle IAM d'opérations par lot que vous avez défini précédemment. Choisissez Suivant.
10. Sous Review (Vérification), vérifiez les paramètres. Si vous voulez apporter des modifications, choisissez Previous (Précédent). Après avoir confirmé les paramètres d'opérations par lot, choisissez Create job (Créer une tâche).

    Pour de plus amples informations, veuillez consulter Création d'une tâche d'opérations par lot S3.

Exécuter votre tâche d'opérations par lot

L'assistant de configuration vous renvoie automatiquement à la section Opérations par lot S3 de la console Amazon S3. Votre nouvelle tâche passe de l'état New (Nouvelle) à l'état Preparing (Préparation) quand S3 commence le processus. Pendant la phase de préparation, S3 lit le manifeste de la tâche, vérifie s'il contient des erreurs, et calcule le nombre d'objets.

1. Choisissez le bouton d'actualisation dans la console Amazon S3 pour vérifier la progression. Selon la taille du manifeste, la lecture peut prendre des minutes ou des heures.
2. Quand S3 finit de lire le manifeste de la tâche, la tâche passe à l'état Awaiting your confirmation (En attente de confirmation). Cliquez sur le bouton d'option à gauche de l'ID de tâche, puis choisissez Run job (Exécuter la tâche).
3. Vérifiez les paramètres de la tâche, puis, dans le coin inférieur droit choisissez Run job (Exécuter la tâche).

   Lorsque la tâche commence à s'exécuter, vous pouvez choisir le bouton d'actualisation pour vérifier sa progression dans l'affichage du tableau de bord de la console ou en sélectionnant la tâche.
4. Une fois la tâche est terminée, vous pouvez afficher le nombre d'objets Succès et Échec pour confirmer que tout a été effectué comme prévu. Si vous avez activé les rapports de tâche, vérifiez dans votre rapport de tâche la cause exacte de toute opération ayant échoué.

Vous pouvez également effectuer ces étapes à l'aide de l'API REST AWS CLI AWS SDKs, ou Amazon S3. Pour plus d'informations sur le suivi de l'état des tâches et les rapports de fin de tâche, consultezSuivi de l'état de la tâche et des rapports de fin de tâche.

Pour des exemples illustrant l'opération de copie avec des balises utilisant le AWS CLI et AWS SDK pour Java, voirCréation d'une tâche d'opérations par lot avec des étiquettes de tâche utilisées pour l'étiquetage.

AWS Lambda Fonction Invoke

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. L'opération Invoke AWS Lambda function Batch Operations lance des AWS Lambda fonctions pour effectuer des actions personnalisées sur des objets répertoriés dans un manifeste. Cette section décrit comment créer une fonction Lambda à utiliser avec des opérations par lot S3 et comment créer une tâche pour invoquer la fonction. La tâche S3 Batch Operations utilise l'opération `LambdaInvoke` pour exécuter une fonction Lambda sur chaque objet répertorié dans un manifeste.

Vous pouvez utiliser S3 Batch Operations à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs Pour plus d'informations sur l'utilisation de Lambda, consultez Mise en route avec AWS Lambda dans le Guide du développeur AWS Lambda .

Les sections suivantes expliquent comment commencer à utiliser les opérations par lot S3 avec Lambda.

Rubriques

- Utilisation de Lambda avec les opérations par lot
- Création d'une fonction Lambda à utiliser avec les opérations par lot S3
- Création d'une tâche d'opérations par lot S3 qui invoque une fonction Lambda
- Fourniture d'informations au niveau des tâches dans les manifestes Lambda
- Tutoriel des opérations par lots S3

Utilisation de Lambda avec les opérations par lot

Lorsque vous utilisez S3 Batch Operations avec AWS Lambda, vous devez créer de nouvelles fonctions Lambda spécifiquement destinées à être utilisées avec S3 Batch Operations. Vous ne

pouvez pas réutiliser les fonctions basées sur des événements Amazon S3 existantes avec les opérations par lot S3. Les fonctions d'événements peuvent seulement recevoir des messages. Elles ne peuvent pas en renvoyer. Les fonctions Lambda utilisées avec les opérations par lot S3 doivent accepter et renvoyer des messages. Pour plus d'informations sur l'utilisation de Lambda avec les événements Amazon S3, consultez la section Utilisation AWS Lambda avec Amazon S3 dans le manuel du AWS Lambda développeur.

Vous créez une tâche d'opérations par lot S3 qui invoque votre fonction Lambda. La tâche exécute la même fonction Lambda pour tous les objets répertoriés dans votre manifeste. Vous pouvez contrôler les versions de votre fonction Lambda à utiliser lors du traitement des objets dans votre manifeste. Les opérations par lots S3 prennent en charge les noms de ressources Amazon (ARNs) non qualifiés, les alias et les versions spécifiques. Pour plus d'informations, consultez la section Introduction au AWS Lambda versionnement dans le guide du AWS Lambda développeur.

Si vous donnez un ARN de fonction qui utilise un alias ou le qualificatif `$LATEST` à la tâche d'opérations par lot S3, et que vous mettez à jour la version vers laquelle l'un de ces points pointe, les opérations par lot S3 commencent à appeler la nouvelle version de votre fonction Lambda. Cela peut être utile lorsque vous souhaitez mettre à jour la fonctionnalité en cours de traitement d'une tâche importante. Si vous ne souhaitez pas que les opérations par lot S3 modifient la version utilisée, indiquez la version spécifique dans le paramètre `FunctionARN` lorsque vous créez la tâche.

Une seule AWS Lambda tâche avec S3 Batch Operations peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

Utilisation de Lambda et des opérations par lot avec des compartiments de répertoires

Les compartiments de répertoires sont un type de compartiment Amazon S3 conçu pour les charges de travail ou les applications critiques en termes de performances qui nécessitent une latence constante inférieure à dix millisecondes. Pour plus d'informations, consultez Compartiments de répertoires.

L'utilisation d'opérations par lots pour invoquer des fonctions Lambda agissant sur des compartiments de répertoires est soumise à des exigences particulières. Par exemple, vous devez structurer votre demande Lambda à l'aide d'un schéma JSON mis à jour et spécifier InvocationSchemaVersion 2.0 (pas 1.0) lorsque vous créez la tâche. Ce schéma mis à jour vous permet de spécifier des paires clé-valeur facultatives pour UserArguments, que vous pouvez utiliser pour modifier certains paramètres des fonctions Lambda existantes. Pour plus d'informations, consultez Automatiser le traitement des objets dans les compartiments d'annuaire Amazon S3 avec S3 Batch Operations et AWS Lambda sur le blog AWS de stockage.

Codes de réponse et de résultat

Les opérations par lot S3 invoquent la fonction Lambda avec une ou plusieurs clés, chacune étant associée à un `TaskID`. Les opérations par lot S3 s'attendent à recevoir un code de résultat par clé de la part des fonctions Lambda. Toute tâche IDs envoyée dans la demande qui n'est pas renvoyée avec un code de résultat par clé recevra le code de résultat indiqué `treatMissingKeysAs` dans le champ. `treatMissingKeysAs`est un champ de demande facultatif dont la valeur par défaut est. `TemporaryFailure` Le tableau suivant contient les autres codes de résultat et valeurs possibles pour le champ `treatMissingKeysAs`.

Code de réponse	Description
`Succeeded`	La tâche s'est achevée normalement. Si vous avez demandé un rapport de fin de tâche, la chaîne de résultat de la tâche est comprise dans le rapport.
`TemporaryFailure`	La tâche a fait l'objet d'un échec temporair e et sera relancée avant la fin de la tâche. La chaîne de résultat est ignorée. Si c'est le relancement final, le message d'erreur est inclus dans le rapport final.
`PermanentFailure`	La tâche a fait l'objet d'un échec permanent. Si vous avez demandé un rapport de fin de tâche, la tâche est marquée comme `Failed` et inclut la chaîne de message d'erreur. Les chaînes de résultats provenant de tâches échouées sont ignorées.

Création d'une fonction Lambda à utiliser avec les opérations par lot S3

Cette section fournit des exemples d'autorisations AWS Identity and Access Management (IAM) que vous devez utiliser avec votre fonction Lambda. Elle contient également un exemple de fonction Lambda à utiliser avec les opérations par lot S3. Si vous n'avez jamais créé de fonction Lambda auparavant, consultez Tutoriel : Utilisation AWS Lambda avec Amazon S3 dans le Guide du AWS Lambda développeur.

Vous devez créer des fonctions Lambda spécifiques à utiliser avec les opérations par lot S3. Vous ne pouvez pas réutiliser les fonctions Lambda basées sur des événements Amazon S3, car les fonctions Lambda utilisées pour les opérations par lot S3 doivent accepter et renvoyer des champs de données spéciaux.

> **Important**
>
> AWS Lambda les fonctions écrites en Java acceptent l'une RequestHandlerou l'autre des RequestStreamHandlerinterfaces de gestion. Cependant, pour prendre en charge le format de demande et de réponse S3 Batch Operations, AWS Lambda il faut une `RequestStreamHandler` interface pour la sérialisation personnalisée et la désérialisation d'une demande et d'une réponse. Cette interface permet à Lambda de transmettre un « InputStream and » OutputStream à la méthode Java`handleRequest`.
> Assurez-vous d'utiliser l'interface `RequestStreamHandler` lorsque vous utilisez les fonctions Lambda avec les opérations par lot S3. Si vous utilisez une interface `RequestHandler`, la tâche par lot échouera avec « JSON non valide retourné dans la charge utile Lambda » dans le rapport de fin.
> Pour plus d'informations, consultez Interfaces du gestionnaire dans le Guide de l'utilisateur AWS Lambda .

Exemples d'autorisations IAM

Voici des exemples d'autorisations IAM nécessaires à l'utilisation d'une fonction Lambda avec les opérations par lot S3.

Example - Stratégie d'approbation des opérations par lot S3.

Voici un exemple de stratégie d'approbation que vous pouvez utiliser pour le rôle IAM des opérations par lot. Ce rôle IAM est spécifié lorsque vous créez la tâche et donne aux opérations par lot l'autorisation d'endosser le rôle IAM.

JSON

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

```
            "Principal": {
                "Service": "batchoperations.s3.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Example - Politique IAM Lambda

Voici un exemple de politique IAM qui donne aux opérations par lot S3 l'autorisation d'invoquer la fonction Lambda et de lire le manifeste d'entrée.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "BatchOperationsLambdaPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:PutObject",
                "lambda:InvokeFunction"
            ],
            "Resource": "*"
        }
    ]
}
```

Exemple de demande et de réponse

Cette section fournit des exemples de demandes et réponses pour la fonction Lambda.

Example Demande

L'exemple suivant est un exemple JSON de requête pour la fonction Lambda.

```
{
```

```
    "invocationSchemaVersion": "1.0",
    "invocationId": "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
    "job": {
        "id": "f3cc4f60-61f6-4a2b-8a21-d07600c373ce"
    },
    "tasks": [
        {
            "taskId": "dGFza2lkZ29lc2hlcmUK",
            "s3Key": "customerImage1.jpg",
            "s3VersionId": "1",
            "s3BucketArn": "arn:aws:s3:us-east-1:0123456788:amzn-s3-demo-bucket1"
        }
    ]
}
```

Example Réponse

L'exemple suivant est un exemple JSON de réponse pour la fonction Lambda.

```
{
  "invocationSchemaVersion": "1.0",
  "treatMissingKeysAs" : "PermanentFailure",
  "invocationId" : "YXNkbGZqYWRmaiBhc2RmdW9hZHNmZGpmaGFzbGtkaGZza2RmaAo",
  "results": [
    {
      "taskId": "dGFza2lkZ29lc2hlcmUK",
      "resultCode": "Succeeded",
      "resultString": "[\"Mary Major", \"John Stiles\"]"
    }
  ]
}
```

Exemple de fonction Lambda pour les opérations par lot S3

L'exemple suivant Python Lambda supprime un marqueur de suppression d'un objet versionné.

Comme l'exemple le montre, les clés des opérations par lot S3 sont encodées par URL. Pour utiliser Amazon S3 avec d'autres AWS services, il est important de décoder par URL la clé transmise par S3 Batch Operations.

```
import logging
from urllib import parse
import boto3
```

```
from botocore.exceptions import ClientError

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

s3 = boto3.client("s3")


def lambda_handler(event, context):
    """
    Removes a delete marker from the specified versioned object.

    :param event: The S3 batch event that contains the ID of the delete marker
                  to remove.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation. When the result code is TemporaryFailure, S3 retries the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None

    task = event["tasks"][0]
    task_id = task["taskId"]

    try:
        obj_key = parse.unquote(task["s3Key"], encoding="utf-8")
        obj_version_id = task["s3VersionId"]
        bucket_name = task["s3BucketArn"].split(":")[-1]

        logger.info(
            "Got task: remove delete marker %s from object %s.", obj_version_id,
 obj_key
        )

        try:
            # If this call does not raise an error, the object version is not a delete
            # marker and should not be deleted.
            response = s3.head_object(
```

```
                Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
            )
            result_code = "PermanentFailure"
            result_string = (
                f"Object {obj_key}, ID {obj_version_id} is not " f"a delete marker."
            )

            logger.debug(response)
            logger.warning(result_string)
        except ClientError as error:
            delete_marker = error.response["ResponseMetadata"]["HTTPHeaders"].get(
                "x-amz-delete-marker", "false"
            )
            if delete_marker == "true":
                logger.info(
                    "Object %s, version %s is a delete marker.", obj_key,
obj_version_id
                )
                try:
                    s3.delete_object(
                        Bucket=bucket_name, Key=obj_key, VersionId=obj_version_id
                    )
                    result_code = "Succeeded"
                    result_string = (
                        f"Successfully removed delete marker "
                        f"{obj_version_id} from object {obj_key}."
                    )
                    logger.info(result_string)
                except ClientError as error:
                    # Mark request timeout as a temporary failure so it will be
retried.
                    if error.response["Error"]["Code"] == "RequestTimeout":
                        result_code = "TemporaryFailure"
                        result_string = (
                            f"Attempt to remove delete marker from  "
                            f"object {obj_key} timed out."
                        )
                        logger.info(result_string)
                    else:
                        raise
            else:
                raise ValueError(
                    f"The x-amz-delete-marker header is either not "
                    f"present or is not 'true'."
```

```
            )
    except Exception as error:
        # Mark all other exceptions as permanent failures.
        result_code = "PermanentFailure"
        result_string = str(error)
        logger.exception(error)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

Création d'une tâche d'opérations par lot S3 qui invoque une fonction Lambda

Lors de la création d'une tâche d'opérations par lot S3 pour appeler une fonction Lambda, vous devez fournir les éléments suivants :

- L'ARN de votre fonction Lambda (qui peut inclure l'alias de fonction ou le numéro de version spécifique)
- Un rôle IAM doté de l'autorisation d'invoquer la fonction
- Le paramètre d'action `LambdaInvokeFunction`

Pour plus d'informations sur la création d'une tâche d'opérations par lots S3, consultez Création d'une tâche d'opérations par lot S3 et Opérations prises en charge par les opérations par lot S3.

L'exemple suivant crée une tâche d'opérations par lot S3 qui invoque une fonction Lambda à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control create-job
    --account-id account-id
    --operation  '{"LambdaInvoke": { "FunctionArn": "arn:aws:lambda:region:account-
id:function:LambdaFunctionName" } }'
    --manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820","Fields":
["Bucket","Key"]},"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-
bucket","ETag":"ManifestETag"}}'
    --report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-
bucket","Format":"Report_CSV_20180820","Enabled":true,"Prefix":"ReportPrefix","ReportScope":"Al
    --priority 2
    --role-arn arn:aws:iam::account-id:role/BatchOperationsRole
    --region region
    --description "Lambda Function"
```

Fourniture d'informations au niveau des tâches dans les manifestes Lambda

Lorsque vous utilisez AWS Lambda des fonctions avec S3 Batch Operations, vous souhaiterez peut-être que des données supplémentaires accompagnent chaque tâche ou clé exécutée. Par exemple, vous pouvez souhaiter que la clé d'objet source et la nouvelle clé d'objet soient fournies. Votre fonction Lambda peut alors copier la clé source vers un nouveau compartiment S3 avec un nouveau nom. Par défaut, les opérations par lot vous permettent de spécifier uniquement le compartiment de destination et une liste de clés source dans le manifeste d'entrée dans votre tâche. Les exemples suivants décrivent comment inclure des données supplémentaires dans le manifeste afin que vous puissiez exécuter des fonctions Lambda plus complexes.

Pour spécifier des paramètres individuels pour chaque clé dans votre manifeste d'opérations par lot S3 à utiliser dans le code de votre fonction Lambda, utilisez le format JSON codé en URL suivant. Le champ `key` est transmis à votre fonction Lambda comme s'il s'agissait d'une clé d'objet Amazon S3. La fonction Lambda peut cependant considérer qu'il contient d'autres valeurs ou plusieurs clés, comme illustré dans les exemples suivants.

> **Note**
>
> Dans le manifeste, le nombre maximal de caractères pour le champ `key` est 1 024.

Example - Manifeste substituant les « clés Amazon S3 » par des chaînes JSON

La version codée URL est fournie aux opérations par lot S3.

```
amzn-s3-demo-bucket,{"origKey": "object1key", "newKey": "newObject1Key"}
amzn-s3-demo-bucket,{"origKey": "object2key", "newKey": "newObject2Key"}
amzn-s3-demo-bucket,{"origKey": "object3key", "newKey": "newObject3Key"}
```

Example - Manifeste codé en URL

Cette version codée en URL doit être fournie aux opérations par lot S3. La non-URL-encoded version ne fonctionne pas.

```
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object1key%22%2C%20%22newKey%22%3A
%20%22newObject1Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object2key%22%2C%20%22newKey%22%3A
%20%22newObject2Key%22%7D
amzn-s3-demo-bucket,%7B%22origKey%22%3A%20%22object3key%22%2C%20%22newKey%22%3A
%20%22newObject3Key%22%7D
```

Example - Fonction Lambda avec format de manifeste écrivant les résultats dans le rapport de la tâche

Cet exemple de manifeste codé par URL contient des clés d'objet délimitées par des barres verticales, que la fonction Lambda suivante doit analyser.

```
amzn-s3-demo-bucket,object1key%7Clower
amzn-s3-demo-bucket,object2key%7Cupper
amzn-s3-demo-bucket,object3key%7Creverse
amzn-s3-demo-bucket,object4key%7Cdelete
```

Cette fonction Lambda montre comment analyser une tâche séparée par une barre verticale, qui est codée dans le manifeste des opérations par lot S3. La tâche indique l'opération de révision qui est appliquée à l'objet spécifié.

```
import logging
from urllib import parse
import boto3
from botocore.exceptions import ClientError

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

s3 = boto3.resource("s3")
```

```
def lambda_handler(event, context):
    """
    Applies the specified revision to the specified object.

    :param event: The Amazon S3 batch event that contains the ID of the object to
                  revise and the revision type to apply.
    :param context: Context about the event.
    :return: A result structure that Amazon S3 uses to interpret the result of the
             operation.
    """
    # Parse job parameters from Amazon S3 batch operations
    invocation_id = event["invocationId"]
    invocation_schema_version = event["invocationSchemaVersion"]

    results = []
    result_code = None
    result_string = None

    task = event["tasks"][0]
    task_id = task["taskId"]
    # The revision type is packed with the object key as a pipe-delimited string.
    obj_key, revision = parse.unquote(task["s3Key"], encoding="utf-8").split("|")
    bucket_name = task["s3BucketArn"].split(":")[-1]

    logger.info("Got task: apply revision %s to %s.", revision, obj_key)

    try:
        stanza_obj = s3.Bucket(bucket_name).Object(obj_key)
        stanza = stanza_obj.get()["Body"].read().decode("utf-8")
        if revision == "lower":
            stanza = stanza.lower()
        elif revision == "upper":
            stanza = stanza.upper()
        elif revision == "reverse":
            stanza = stanza[::-1]
        elif revision == "delete":
            pass
        else:
            raise TypeError(f"Can't handle revision type '{revision}'.")

        if revision == "delete":
            stanza_obj.delete()
            result_string = f"Deleted stanza {stanza_obj.key}."
```

```
        else:
            stanza_obj.put(Body=bytes(stanza, "utf-8"))
            result_string = (
                f"Applied revision type '{revision}' to " f"stanza {stanza_obj.key}."
            )

        logger.info(result_string)
        result_code = "Succeeded"
    except ClientError as error:
        if error.response["Error"]["Code"] == "NoSuchKey":
            result_code = "Succeeded"
            result_string = (
                f"Stanza {obj_key} not found, assuming it was deleted "
                f"in an earlier revision."
            )
            logger.info(result_string)
        else:
            result_code = "PermanentFailure"
            result_string = (
                f"Got exception when applying revision type '{revision}' "
                f"to {obj_key}: {error}."
            )
            logger.exception(result_string)
    finally:
        results.append(
            {
                "taskId": task_id,
                "resultCode": result_code,
                "resultString": result_string,
            }
        )
    return {
        "invocationSchemaVersion": invocation_schema_version,
        "treatMissingKeysAs": "PermanentFailure",
        "invocationId": invocation_id,
        "results": results,
    }
```

Tutoriel des opérations par lots S3

Le didacticiel suivant présente des end-to-end procédures complètes pour certaines tâches d'opérations par lots avec Lambda. Dans ce didacticiel, vous apprendrez à configurer les opérations par lot S3 pour invoquer une fonction Lambda pour le transcodage par lot de vidéos stockées dans un compartiment source S3. La fonction Lambda appelle AWS Elemental MediaConvert pour transcoder les vidéos.

- Didacticiel : transcodage par lot de vidéos avec les opérations par lot S3

Replace all object tags (Remplacer toutes les étiquettes des objets)

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. L'opération Remplacer toutes les balises d'objet remplace les balises de chaque objet répertorié dans le manifeste. Une balise d'objet est une paire clé/valeur de chaînes que vous pouvez utiliser pour stocker les métadonnées relatives à un objet.

Pour créer une tâche de remplacement de toutes les balises d'objet, vous devez fournir un ensemble de balises à appliquer. S3 Batch Operations applique le même ensemble d'étiquettes à chaque objet. Le jeu d'étiquettes que vous fournissez remplace les jeux d'étiquettes déjà associés aux objets du manifeste. Les opérations par lot S3 ne permettent pas d'ajouter des balises aux objets tout en laissant les balises existantes en place.

Si les objets de votre manifeste se trouvent dans un compartiment versionné, vous pouvez appliquer l'ensemble d'étiquettes à des versions spécifiques de chaque objet. Pour ce faire, spécifiez un ID de version pour chaque objet dans le manifeste. Si vous n'incluez pas d'ID de version pour les objets, les opérations par lot S3 applique l'ensemble de balises à la dernière version de l'objet. Pour plus d'informations sur les manifestes Batch Operations, consultez Spécification d'un manifeste.

Pour plus d'informations sur le balisage d'objets, consultez Catégorisation de vos objets à l'aide de balises dans ce guide. Consultez aussi PutObjectTagging, GetObjectTagging et DeleteObjectTagging dans la Référence d'API Amazon Simple Storage Service.

Pour utiliser la console afin de créer une tâche Remplacer toutes les balises d'objets, consultez Création d'une tâche d'opérations par lot S3.

Restrictions et limitations

Lorsque vous utilisez les opérations par lot pour remplacer des balises d'objet, les restrictions et limites suivantes s'appliquent :

- Le rôle AWS Identity and Access Management (IAM) que vous spécifiez pour exécuter la tâche Batch Operations doit disposer des autorisations nécessaires pour effectuer l'`PutObjectTagging`opération sous-jacente. Pour plus d'informations sur les autorisations nécessaires, consultez PutObjectTagging dans la Référence d'API Amazon Simple Storage Service.
- Les opérations par lot S3 utilisent l'opération Amazon S3 PutObjectTagging pour appliquer des balises à chaque objet du manifeste. Toutes les restrictions et limitations qui s'appliquent à l'opération sous-jacente s'appliquent également aux tâches S3 Batch Opérations.
- Une seule tâche de remplacement de toutes les balises d'objets peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

Delete all object tags (Supprimer toutes les étiquettes des objets)

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. L'opération Delete all object tags (Supprimer toutes les étiquettes des objets) supprime tous les ensembles de étiquettes Amazon S3 associés aux objets répertoriés dans le manifeste. Les opérations par lot S3 ne permettent pas de supprimer des balises d'objet tout en conservant les autres balises en place.

Si les objets de votre manifeste se trouvent dans un compartiment versionné, vous pouvez supprimer les ensembles d'étiquettes d'une version d'un objet. Pour ce faire, vous devez spécifier un ID de version pour chaque objet dans le manifeste. Si vous n'incluez pas d'ID de version pour un objet, S3 Batch Operations supprime l'ensemble d'étiquettes de la dernière version de chaque objet. Pour plus d'informations sur les manifestes Batch Operations, consultez Spécification d'un manifeste.

Pour plus d'informations sur le balisage des objets, consultez Catégorisation de vos objets à l'aide de balises dans ce guide ainsi que PutObjectTagging, GetObjectTagging et DeleteObjectTagging dans la Référence d'API Amazon Simple Storage Service.

> **Warning**
>
> L'exécution de cette tâche supprime tous les ensembles d'étiquettes sur chaque objet répertorié dans le manifeste.

Pour utiliser la console afin de créer une tâche Supprimer toutes les balises d'objet, consultez Création d'une tâche d'opérations par lot S3.

Restrictions et limitations

Lorsque vous utilisez les opérations par lot pour supprimer des balises d'objets, les restrictions et limites suivantes s'appliquent :

- Le rôle AWS Identity and Access Management (IAM) que vous spécifiez pour exécuter la tâche doit disposer des autorisations nécessaires pour effectuer l'`DeleteObjectTagging`opération Amazon S3 sous-jacente. Pour plus d'informations, consultez DeleteObjectTagging dans la Référence d'API Amazon Simple Storage Service.
- Les opérations par lot S3 utilisent l'opération Amazon S3 DeleteObjectTagging pour supprimer les ensembles de balises de chaque objet du manifeste. Toutes les restrictions et limitations qui s'appliquent à l'opération sous-jacente s'appliquent également aux tâches S3 Batch Opérations.
- Une seule tâche de suppression du balisage d'objets peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

Remplacer une liste de contrôle d'accès (ACL)

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. L'opération Remplacer la liste de contrôle d'accès (ACL) remplace les listes de contrôle d'accès (ACLs) pour chaque objet répertorié dans le manifeste. En utilisant ACLs, vous pouvez définir les personnes autorisées à accéder à un objet et les actions qu'elles peuvent effectuer.

> **Note**
>
> La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

S3 Batch Operations prend en charge les autorisations personnalisées ACLs que vous définissez et les ACLs versions prédéfinies fournies par Amazon S3 avec un ensemble prédéfini d'autorisations d'accès.

Si les objets de votre manifeste se trouvent dans un compartiment versionné, vous pouvez les appliquer ACLs à des versions spécifiques de chaque objet. Pour ce faire, spécifiez un ID de version pour chaque objet dans le manifeste. Si vous n'incluez aucun ID de version pour les objets, les opérations par lot S3 appliquent la liste de contrôle d'accès à la dernière version de l'objet.

Pour plus d'informations sur ACLs Amazon S3, consultezPrésentation de la liste de contrôle d'accès (ACL).

S3 Block Public Access

Si vous souhaitez limiter l'accès public à tous les objets d'un compartiment, nous vous recommandons d'utiliser Amazon S3 Block Public Access au lieu d'utiliser S3 Batch Operations pour vous appliquer ACLs. Le blocage de l'accès publique permet de limiter l'accès par compartiment ou par compte via une seule opération simple et rapide. Le blocage de l'accès public Amazon S3 est préférable lorsque votre objectif est de contrôler l'accès public à tous les objets d'un compartiment ou d'un compte. N'utilisez les opérations par lot S3 que lorsque vous devez appliquer une liste de contrôle d'accès (ACL) prédéfinie à chaque objet du manifeste. Pour de plus amples informations sur le blocage de l'accès public S3, consultez Blocage de l'accès public à votre stockage Amazon S3.

Propriété de l'objet S3

Si les objets du manifeste se trouvent dans un compartiment qui utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets, l'opération Remplacer la liste de contrôle d'accès (ACL) peut uniquement spécifier un objet ACLs qui accorde un contrôle total au propriétaire du compartiment. Dans ce cas, l'opération Remplacer la liste de contrôle d'accès (ACL) ne peut pas accorder d'autorisations ACL d'objets à d'autres Comptes AWS ou à des groupes. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Restrictions et limitations

Lorsque vous utilisez Batch Operations pour remplacer ACLs, les restrictions et limitations suivantes s'appliquent :

- Le rôle AWS Identity and Access Management (IAM) que vous spécifiez pour exécuter la tâche de remplacement de la liste de contrôle d'accès (ACL) doit disposer des autorisations nécessaires pour effectuer l'`PutObjectAcl`opération Amazon S3 sous-jacente. Pour plus d'informations sur les autorisations nécessaires, consultez PutObjectAcl dans la Référence d'API Amazon Simple Storage Service.

- Les opérations par lot S3 utilisent l'opération Amazon S3 `PutObjectAcl` pour appliquer la liste de contrôle d'accès ACL spécifiée à chaque objet du manifeste. Par conséquent, toutes les restrictions et limites qui s'appliquent à l'opération `PutObjectAcl` sous-jacente s'appliquent également aux tâches d'opérations par lot S3 Remplacer une liste de contrôle d'accès (ACL).
- Une seule tâche de remplacement de liste de contrôle d'accès peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

Restauration d'objets à l'aide d'opérations par lot

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. L'opération Restaurer lance des demandes de restauration pour les objets Amazon S3 archivés, répertoriés dans votre manifeste. Les objets archivés suivants doivent être restaurés pour qu'il soit possible d'y accéder en temps réel :

- Objets archivés dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive
- Objets archivés via la classe de stockage S3 Intelligent-Tiering dans les niveaux Archive Access ou Deep Archive Access

L'utilisation d'une opération Restaurer (S3InitiateRestoreObjectOperation) dans votre tâche d'opérations par lot S3 entraîne une demande `RestoreObject` pour chaque objet spécifié dans le manifeste.

> **Important**
>
> La tâche Restaurer initie uniquement la demande de restauration d'objets. S3 Batch Operations indique que la tâche est terminée pour chaque objet après que la demande a été lancée pour l'objet. Amazon S3 ne met pas à jour la tâche ou ne vous avertit pas lorsque les objets ont été restaurés. Toutefois, vous pouvez utiliser des notifications d'événements S3 pour recevoir des notifications lorsque les objets sont disponibles dans Amazon S3. Pour de plus amples informations, veuillez consulter Notifications d'événements Amazon S3.

Lorsque vous créez une tâche Restaurer, les arguments suivants sont disponibles :

ExpirationInDays

Cet argument spécifie combien de temps l'objet S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive reste disponible dans Amazon S3. Les tâches Restaurer qui ciblent des objets S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive exigent que vous définissiez `ExpirationInDays` sur 1 ou plus.

> **Important**
>
> Ne définissez pas `ExpirationInDays` lors de la création de tâches d'opération Restaurer, qui ciblent des objets de niveau Archive Access ou Deep Archive Access de S3 Intelligent-Tiering. Les objets des niveaux Archive Access de S3 Intelligent-Tiering ne sont pas soumis à l'expiration de la restauration. Par conséquent, spécifier `ExpirationInDays` entraîne un échec de la demande `RestoreObject`.

GlacierJobTier

Amazon S3 peut restaurer des objets en utilisant un des trois niveaux de récupération suivants : `EXPEDITED`, `STANDARD` ou `BULK`. Toutefois, la fonction S3 Batch Operations prend en charge uniquement les niveaux de récupération `STANDARD` et `BULK`. Pour plus d'informations sur les différences entre les niveaux de récupération, consultez Présentation des options de récupération d'archives.

Pour plus d'informations sur la tarification de chaque niveau, consultez la section Demandes et récupérations de données dans la page Tarification Amazon S3.

Différences entre la restauration depuis S3 Glacier et S3 Intelligent-Tiering

La restauration de fichiers archivés à partir des classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive diffère de la restauration de fichiers de la classe de stockage S3 Intelligent-Tiering dans les niveaux d'accès Archive ou Deep Archive.

- Lorsque vous effectuez une restauration à partir de S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, une copie temporaire de l'objet est créée. Amazon S3 supprime cette copie après l'expiration de la valeur que vous avez spécifiée dans l'argument `ExpirationInDays`. Une fois la copie temporaire supprimée, vous devez soumettre une demande de restauration supplémentaire pour accéder à l'objet.

- Lors de la restauration d'objets S3 Intelligent-Tiering archivés, ne spécifiez pas l'argument `ExpirationInDays`. Lorsque vous restaurez un objet depuis le niveau Archive Access ou Deep Archive Access de S3 Intelligent-Tiering, l'objet repasse au niveau d'accès fréquent de S3 Intelligent-Tiering. Après un minimum de 90 jours consécutifs sans accès, l'objet passe automatiquement au niveau Archive Access. Après un minimum de 180 jours consécutifs sans accès, l'objet passe automatiquement au niveau Deep Archive Access.
- Les tâches d'opérations par lot peuvent fonctionner sur les objets de classe de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive, ou sur les objets des niveaux de stockage Archive Access et Deep Archive Access de S3 Intelligent-Tiering. Les opérations par lot ne peuvent pas fonctionner sur les deux types d'objets archivés dans la même tâche. Pour restaurer des objets des deux types, vous devez créer des tâches Batch Operations.

Chevauchement de restaurations

Si la tâche S3InitiateRestoreObjectOperation essaie de restaurer un objet dont la restauration est déjà en cours, les opérations par lot S3 procèdent comme suit.

La restauration de l'objet aboutit si l'une des conditions suivantes est vraie :

- Comparée à la demande de restauration en cours, la valeur `ExpirationInDays` de cette tâche est la même et sa valeur `GlacierJobTier` est plus rapide.
- La demande de restauration précédente est déjà terminée, et l'objet est actuellement disponible. Dans ce cas, les opérations par lot mettent à jour la date d'expiration de l'objet restauré pour qu'elle corresponde à la valeur `ExpirationInDays` spécifiée dans la demande de restauration en cours.

L'opération de restauration échoue pour l'objet si l'une des conditions suivantes est vraie :

- La demande de restauration en cours n'est pas encore terminée, et la durée de restauration de cette tâche (spécifiée par la valeur `ExpirationInDays`) diffère de la durée de restauration spécifiée dans la demande de restauration en cours.
- Le niveau de restauration de cette tâche (spécifié par la valeur `GlacierJobTier`) est inférieur ou égal au niveau de restauration spécifié dans la demande de restauration en cours.

Limites

Les tâches `S3InitiateRestoreObjectOperation` présentent les limites suivantes :

- Vous devez créer la tâche dans la même Région que les objets archivés.
- Les opérations par lot S3 ne prennent pas en charge le niveau d'extraction `EXPEDITED`.
- Une seule tâche de restauration des opérations par lots peut prendre en charge un manifeste contenant jusqu'à 4 milliards d'objets.

Pour plus d'informations sur la restauration des objets, consultez Restauration d'un objet archivé.

Conservation d'un verrouillage d'objet S3

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. Vous pouvez utiliser l'opération de Rétention Verrouillage d'objet pour appliquer des dates de rétention à vos objets en mode gouvernance ou en mode conformité. Ces modes de rétention appliquent différents niveaux de protection. Vous pouvez appliquer l'un ou l'autre des modes de rétention à n'importe quelle version d'objet. Les dates de rétention, comme les conservations légales, empêchent l'écrasement ou la suppression d'un objet. Amazon S3 stocke la date de fin de rétention (Rétention jusqu'à la date) spécifiée dans les métadonnées de l'objet et protège la version spécifiée de cette version de l'objet jusqu'à l'expiration de la période de rétention.

Vous pouvez utiliser les opérations par lot S3 avec le verrouillage d'objet pour gérer simultanément les dates de rétention de nombreux objets Amazon S3. Vous spécifiez la liste des objets cibles dans votre manifeste et l'envoyez aux tâches d'opérations par lot pour les finaliser. Pour plus d'informations, consultez Verrouillage d'objet S3 the section called "Périodes de rétention".

Votre tâche d'opérations par lot S3 avec des dates de conservation s'exécute jusqu'à la fin, jusqu'à son annulation ou jusqu'à ce qu'un état d'échec soit atteint. Nous vous recommandons d'utiliser les opérations par lot S3 et la rétention du verrouillage d'objet S3 lorsque vous souhaitez ajouter, modifier ou supprimer la date de rétention de nombreux objets avec une seule demande.

Les opérations par lot vérifient que le verrouillage d'objet est activé sur votre compartiment avant de traiter les clés du manifeste. Pour effectuer les opérations et la validation, Batch Operations a besoin des `s3:PutObjectRetention` autorisations `s3:GetBucketObjectLockConfiguration` et d'un rôle AWS Identity and Access Management (IAM) pour permettre à Batch Operations d'appeler Object Lock en votre nom. Pour de plus amples informations, veuillez consulter the section called "Considérations relatives au verrouillage d'objet".

Pour plus d'informations sur l'utilisation de cette opération avec l'API REST, consultez `S3PutObjectRetention` dans l'opération CreateJob dans la Référence d'API Amazon Simple Storage Service.

Pour un exemple AWS Command Line Interface (AWS CLI) d'utilisation de cette opération, voirthe section called "Utiliser les tâches d'opérations par lot avec la rétention du verrouillage des objets". Pour un AWS SDK pour Java exemple, voirthe section called "Utiliser les tâches d'opérations par lot avec la rétention du verrouillage des objets".

Restrictions et limitations

Lorsque vous utilisez les opérations par lot pour appliquer des périodes de conservation du verrouillage d'objet, les restrictions et limites suivantes s'appliquent :

- Les opérations par lot S3 n'apportent aucune modification au niveau du compartiment.
- La gestion des versions et le verrouillage d'objet S3 doivent être configurés sur le compartiment où la tâche est effectuée.
- Tous les objets répertoriés dans le manifeste doivent se trouver dans le même compartiment.
- L'opération fonctionne sur la dernière version de l'objet, sauf si une version est explicitement spécifiée dans le manifeste.
- Vous avez besoin d'une autorisation `s3:PutObjectRetention` dans votre rôle IAM pour utiliser une tâche de Rétention Verrouillage d'objet.
- L'autorisation IAM `s3:GetBucketObjectLockConfiguration` est nécessaire pour confirmer que le verrouillage d'objet est activé pour le compartiment S3 pour lequel vous effectuez cette tâche.
- Vous ne pouvez prolonger la période de rétention des objets qu'avec des dates de rétention en mode `COMPLIANCE` appliquées. Cette période de rétention ne peut pas être raccourcie.
- Une seule tâche de rétention S3 Object Lock peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

Mise en suspens juridique du verrouillage des objets S3

Vous pouvez utiliser les opérations par lot Amazon S3 pour effectuer des opérations par lot à grande échelle au niveau d'objets Amazon S3. Vous pouvez utiliser l'opération Conservation légale du verrouillage d'objet pour activer la conservation légale d'une version d'objet. À l'instar d'une période de rétention, une conservation légale empêche une version d'objet d'être remplacée ou supprimée.

Cependant, une conservation légale n'est associée à aucune période de rétention et reste en vigueur jusqu'à sa suppression.

Vous pouvez utiliser les opérations par lot S3 avec le verrouillage d'objet pour ajouter des conservations légales à plusieurs objets Amazon S3 à la fois. Pour ce faire, spécifiez une liste des objets cibles dans votre manifeste et envoyez cette liste aux opérations par lot. Votre tâche d'opérations par lot S3 Conservation légale du verrouillage d'objet s'exécute jusqu'à la fin, jusqu'à son annulation ou jusqu'à ce qu'un état d'échec soit atteint.

Les opérations par lot S3 vérifient que le verrouillage d'objet est activé sur votre compartiment S3 avant de traiter les objets du manifeste. Pour effectuer les opérations sur les objets et la validation au niveau du compartiment, S3 Batch Operations a besoin du rôle `s3:PutObjectLegalHold` and `s3:GetBucketObjectLockConfiguration` in an AWS Identity and Access Management (IAM). Ces autorisations permettent aux opérations par lot S3 d'appeler le verrouillage d'objet S3 en votre nom.

Lorsque vous créez la tâche d'opérations par lot S3 pour supprimer la conservation légale, il vous suffit de spécifier `Off` comme statut de la conservation légale. Pour de plus amples informations, veuillez consulter the section called "Considérations relatives au verrouillage d'objet".

Pour plus d'informations sur l'utilisation de cette opération avec l'API REST, consultez `S3PutObjectLegalHold` dans l'opération CreateJob dans la Référence d'API Amazon Simple Storage Service.

Pour un exemple d'utilisation de cette opération, consultez Utilisation du AWS SDK pour Java.

Restrictions et limitations

Lorsque vous utilisez les opérations par lot pour appliquer ou supprimer une conservation légale du verrouillage d'objet, les restrictions et limites suivantes s'appliquent :

- Les opérations par lot S3 n'apportent aucune modification au niveau du compartiment.
- Tous les objets répertoriés dans le manifeste doivent se trouver dans le même compartiment.
- La gestion des versions et le verrouillage d'objet S3 doivent être configurés sur le compartiment où la tâche est effectuée.
- L'opération Conservation légale du verrouillage d'objet fonctionne sur la dernière version de l'objet, sauf si une version est explicitement spécifiée dans le manifeste.
- L'autorisation `s3:PutObjectLegalHold` est nécessaire dans votre rôle IAM pour ajouter ou supprimer une conservation légale des objets.

- L'autorisation IAM `s3:GetBucketObjectLockConfiguration` est nécessaire pour confirmer que le verrouillage d'objet est activé pour le compartiment S3 pour lequel vous effectuez cette tâche.
- Une seule tâche de conservation légale dans S3 Object Lock peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

- Copie d'objets
- AWS Lambda Fonction Invoke
- Replace all object tags (Remplacer toutes les étiquettes des objets)
- Delete all object tags (Supprimer toutes les étiquettes des objets)
- Remplacer une liste de contrôle d'accès (ACL)
- Restauration d'objets à l'aide d'opérations par lot
- Conservation d'un verrouillage d'objet S3
- Mise en suspens juridique du verrouillage des objets S3
- Réplication d'objets existants via la réplication par lot

Gestion des tâches d'opérations par lot S3

Simple Storage Service (Amazon S3) fournit un ensemble d'outils puissants pour vous aider à gérer vos tâches d'opérations par lot S3 après les avoir créées. Cette section décrit les opérations que vous pouvez utiliser pour gérer et suivre vos tâches à l'aide de la console Amazon S3 AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

Rubriques

- Utilisation de la console Simple Storage Service (Amazon S3) pour gérer vos tâches d'opérations par lot S3
- Liste des tâches
- Affichage des détails de la tâche
- Affectation d'une priorité de tâche

Utilisation de la console Simple Storage Service (Amazon S3) pour gérer vos tâches d'opérations par lot S3

À l'aide de la console, vous pouvez gérer vos tâches d'opérations par lot S3. Par exemple, vous pouvez :

- Afficher les tâches actives et mises en file d'attente
- Modifier la priorité d'une tâche
- Confirmer et exécuter une tâche
- Cloner une tâche
- Annuler une tâche

Pour gérer les opérations par lot via la console

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Batch Operations (Opérations par lot).
3. Sélectionnez la tâche que vous souhaitez gérer.

Liste des tâches

Vous pouvez récupérer une liste des tâches d'opérations par lot S3. Cette liste inclut les tâches qui ne sont pas encore terminé, ainsi que celles terminées au cours des 90 derniers jours. La liste des tâches inclut des informations pour chacune des tâches telles que l'ID, la description, la priorité, le statut actuel et le nombre de tâches réussies ou ayant échoué. Vous pouvez filtrer la liste de tâches par statut. Lorsque vous procédez à l'extraction d'une liste des tâches via la console, vous pouvez également rechercher vos tâches par description ou ID et les filtrer par Région AWS.

Génération d'une liste des tâches **`Active`** et **`Complete`**

L' AWS CLI exemple suivant permet d'obtenir une liste de `Complete` tâches `Active` et. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control list-jobs \
    --region us-west-2 \
    --account-id account-id \
    --job-statuses '["Active","Complete"]' \
```

```
    --max-results 20
```

Pour plus d'informations et des exemples, consultez list-jobs dans la Référence des commandes AWS CLI .

Affichage des détails de la tâche

Si vous souhaitez obtenir d'autres d'informations sur une tâche d'opérations par lot Amazon S3 que celles fournies par la liste des tâches, vous pouvez afficher tous les détails d'une seule tâche. Vous pouvez consulter les détails des tâches qui n'ont pas encore été achevées ou qui ont été achevées au cours des 90 derniers jours. Outre les informations renvoyées dans la liste de tâches, les détails d'une seule tâche incluent d'autres éléments, tels que les suivants :

- Paramètres de fonctionnement
- Détails sur le manifeste
- Informations sur le rapport de fin de tâche (si vous en avez configuré un au moment de créer la tâche)
- Le nom de ressource Amazon (ARN) du rôle d'utilisateur AWS Identity and Access Management (IAM) que vous avez attribué pour exécuter la tâche

En affichant les détails d'une tâche individuelle, vous pouvez accéder à la totalité de la configuration d'une tâche. Pour consulter les détails d'une tâche, vous pouvez utiliser la console Amazon S3 ou le AWS Command Line Interface (AWS CLI).

Obtenir la description d'une tâche d'opérations par lot S3 dans la console Amazon S3

Pour afficher la description d'une tâche d'opérations par lot à l'aide de la console

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Opérations par lot.
3. Choisissez l'ID de la tâche spécifique pour en afficher les détails.

Obtenez une description du poste de S3 Batch Operations dans le AWS CLI

L'exemple suivant permet d'obtenir la description d'une tâche d'opérations par lot S3 à l'aide de l' AWS CLI. Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

```
aws s3control describe-job \
--region us-west-2 \
--account-id account-id \
--job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

Pour plus d'informations et des exemples, consultez describe-job dans la Référence des commandes AWS CLI .

Affectation d'une priorité de tâche

Vous pouvez attribuer à chaque tâche d'opérations par lot Amazon S3 une priorité numérique, qui peut être n'importe quel entier positif. Les opérations par lot S3 classent les tâches par ordre de priorité en fonction de la priorité attribuée. Les tâches avec une priorité élevée (ou une valeur d'entier supérieure pour le paramètre de priorité) sont évaluées en premier. La priorité est déterminée par ordre décroissant. Par exemple, une file d'attente de tâches avec une valeur de priorité 10 se voit accorder la préférence en termes de planification par rapport à une file d'attente de tâches avec une valeur de priorité 1.

Vous pouvez modifier la priorité d'une tâche pendant son exécution. Si vous envoyez une nouvelle tâche avec une priorité supérieure alors qu'une tâche est en cours d'exécution, la tâche avec la priorité inférieure peut s'interrompre pour permettre à la tâche avec la priorité supérieure de s'exécuter.

La modification de la priorité d'une tâche n'affecte pas sa vitesse de traitement.

> **Note**
>
> Les opérations par lot S3 respectent les priorités de tâche dans la mesure du possible. Bien que les tâches avec des priorités supérieures soient généralement prioritaires sur les tâches avec des priorités inférieures, Amazon S3 ne garantit pas un ordre strict des tâches.

Utilisation de la console S3

Comment mettre à jour la priorité des tâches dans la console Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Batch Operations (Opérations par lot).

3. Sélectionnez la tâche spécifique que vous souhaitez gérer.
4. Choisissez Actions. Dans la liste déroulante, choisissez Update priority (Mettre à jour la priorité).

À l'aide du AWS CLI

L'exemple suivant met à jour la priorité de la tâche à l'aide de l' AWS CLI. Un nombre plus élevé indique une priorité d'exécution plus élevée. Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

```
aws s3control update-job-priority \
    --region us-west-2 \
    --account-id account-id \
    --priority 98 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c
```

À l'aide du AWS SDK pour Java

L'exemple suivant met à jour la priorité d'une tâche d'opérations par lot S3 à l'aide du kit AWS SDK pour Java.

Pour plus d'informations sur la priorité des tâches, consultez Affectation d'une priorité de tâche.

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobPriorityRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobPriority {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";
```

```
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobPriority(new UpdateJobPriorityRequest()
                    .withAccountId(accountId)
                    .withJobId(jobId)
                    .withPriority(98));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Suivi de l'état de la tâche et des rapports de fin de tâche

Grâce aux opérations par lot S3, vous pouvez afficher et mettre à jour l'état d'une tâche, ajouter des notifications et effectuer la journalisation, suivre les échecs de tâche et générer des rapports de fin de tâches.

Rubriques

- Statuts de la tâche
- Mise à jour de l'état
- Notifications et journalisation
- Suivi de l'échec d'une tâche
- Rapports de fin de tâche
- Exemples : suivi d'une tâche S3 Batch Operations sur Amazon EventBridge via AWS CloudTrail
- Exemples : Rapports de fin de tâche d'opérations par lot S3

Statuts de la tâche

Après la création et l'exécution d'une tâche, celle-ci passe par une série d'états. Le tableau suivant décrit les états et les transitions possibles entre eux.

État	Description	Transitions
`New`	Une tâche commence à l'état `New` lorsque vous la créez.	Une tâche passe automatiquement au statut `Preparing` quand Amazon S3 commence à traiter l'objet de manifeste.
`Preparing`	Amazon S3 traite l'objet manifeste et d'autres paramètres de tâche pour configurer et exécuter la tâche.	Une tâche passe automatiquement au statut `Ready` une fois qu'Amazon S3 a terminé de traiter l'objet de manifeste et les autres paramètres. La tâche peut ensuite exécuter l'opération spécifiée pour les objets répertoriés dans le manifeste. Si la tâche nécessite une confirmation avant l'exécution, ce qui est, par exemple, le cas lors de la création d'une tâche avec la console Amazon S3, celle-ci passe du statut `Preparing` à `Suspended`. Elle reste dans l'état `Suspended` jusqu'à ce que vous confirmiez son exécution.
`Suspended`	La tâche nécessite que vous confirmiez son exécution. Seules les tâches créées	Une fois que vous confirmez que vous souhaitez exécuter

État	Description	Transitions
	avec la console Amazon S3 nécessitent une confirmat ion. Une tâche créée à l'aide de la console passe à l'état `Suspended` juste après `Preparing` . Une fois que vous confirmez que vous souhaitez exécuter la tâche et que la tâche passe à l'était `Ready`, elle ne revient jamais à l'état `Suspended` .	la tâche, son état devient `Ready`.
`Ready`	Amazon S3 peut commencer à exécuter les opérations demandées pour les objets.	Une tâche passe automatiq uement au statut `Active` quand Amazon S3 commence à l'exécuter. La durée pendant laquelle une tâche reste dans l'état `Ready` dépend du niveau de priorité et de la durée des autres tâches qui sont déjà en cours d'exécution.
`Active`	Amazon S3 effectue l'opérati on demandée pour les objets répertoriés dans le manifeste . Pendant qu'une tâche est en cours`Active`, vous pouvez suivre sa progression à l'aide de la console Amazon S3 ou de l'`DescribeJob` opération via l'API REST AWS CLI, ou AWS SDKs.	Une tâche quitte l'état `Active` lorsque plus aucune opération n'est exécutée sur les objets. Ce comportement peut se produire automatiquement, par exemple lorsqu'une tâche aboutit ou échoue. Ce comportement peut également être le résultat d'une action utilisateur, telle que l'annulat ion d'une tâche. L'état dans lequel passe la tâche dépend de la raison de la transition.

État	Description	Transitions
`Pausing`	La tâche passe d'un certain état à `Paused`.	Une tâche passe automatiquement à l'état `Paused` quand l'étape `Pausing` est terminée.
`Paused`	Une tâche peut passer à l'état `Paused` si vous soumettez une autre tâche de priorité plus élevée alors que cette tâche est exécutée.	Une tâche `Paused` retourne automatiquement à l'état `Active` lorsque les tâches de priorité plus élevée qui bloquent l'exécution de cette tâche se terminent, échouent ou sont suspendues.
`Complete`	La tâche a fini d'effectuer l'opération demandée sur tous les objets répertoriés dans le manifeste. L'opération peut avoir abouti ou échoué pour chaque objet. Si vous avez configuré la tâche de sorte à générer un rapport de fin de tâche, ce rapport est disponible dès que la tâche passe à l'état `Complete`.	`Complete` est un état final. Une fois qu'une tâche atteint l'état `Complete`, elle ne passe plus à aucun autre état.
`Cancelling`	La tâche passe à l'état `Cancelled` .	Une tâche passe automatiquement à l'état `Cancelled` quand l'étape `Cancelling` est terminée.
`Cancelled`	Vous avez demandé que la tâche soit annulée, ce qui a été fait par les opérations par lot S3. Cette tâche n'enverra plus de nouvelles demandes à Amazon S3.	`Cancelled` est un état final. Après qu'une tâche atteint l'état `Cancelled` , elle ne passe plus à aucun autre état.

État	Description	Transitions
`Failing`	La tâche passe à l'état `Failed`.	Une tâche passe automatiquement à l'état `Failed` une fois que l'étape `Failing` est terminée.
`Failed`	La tâche a échoué et n'est plus en cours d'exécution. Pour de plus amples informations sur les échecs de tâche, consultez Suivi de l'échec d'une tâche.	`Failed` est un état final. Après qu'une tâche atteint l'état `Failed`, elle ne passe plus à aucun autre état.

Mise à jour de l'état

Les AWS SDK pour Java exemples suivants AWS CLI mettent à jour le statut d'une tâche Batch Operations. Pour plus d'informations sur l'utilisation de la console Amazon S3 pour gérer les tâches d'opérations par lot, consultez Utilisation de la console Simple Storage Service (Amazon S3) pour gérer vos tâches d'opérations par lot S3.

À l'aide du AWS CLI

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

- Si vous n'avez pas spécifié le paramètre `--no-confirmation-required` dans la commande `create-job` précédente, la tâche reste à l'état suspendu jusqu'à ce que vous confirmiez cette tâche en définissant son statut sur `Ready`. Amazon S3 rend ensuite la tâche éligible à l'exécution.

```
aws s3control update-job-status \
    --region us-west-2 \
    --account-id 123456789012 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
    --requested-job-status 'Ready'
```

- Annulez la tâche en définissant son statut sur `Cancelled`.

```
aws s3control update-job-status \
```

```
    --region us-west-2 \
    --account-id 123456789012 \
    --job-id 00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c \
    --status-update-reason "No longer needed" \
    --requested-job-status Cancelled
```

Utilisation du AWS SDK pour Java

L'exemple suivant met à jour le statut d'une tâche d'opérations par lot S3 à l'aide du kit AWS SDK pour Java.

Pour de plus amples informations sur l'état d'une tâche, consultez Suivi de l'état de la tâche et des rapports de fin de tâche.

Example

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.UpdateJobStatusRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateJobStatus {
    public static void main(String[] args) {
        String accountId = "Account ID";
        String jobId = "00e123a4-c0d8-41f4-a0eb-b46f9ba5b07c";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.updateJobStatus(new UpdateJobStatusRequest()
                    .withAccountId(accountId)
```

```
                    .withJobId(jobId)
                    .withRequestedJobStatus("Ready"));

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Notifications et journalisation

En plus de demander des rapports de fin de tâche, vous pouvez également capturer, examiner et auditer l'activité des opérations par lot à l'aide d' AWS CloudTrail. Puisque les opérations par lot utilisent des opérations d'API Amazon S3 existantes pour exécuter des tâches, ces dernières émettent également les mêmes événements que si vous les appeliez directement. Dès lors, vous pouvez suivre et enregistrer la progression de votre tâche et l'ensemble de ses tâches à l'aide des mêmes outils et processus de notification, de journalisation et d'audit que vous utilisez déjà avec Amazon S3. Pour plus d'informations, consultez les exemples dans les sections suivantes.

> **Note**
>
> Batch Operations génère à la fois des événements de gestion et des événements de données CloudTrail pendant l'exécution des tâches. Le volume de ces événements évolue avec le nombre de clés dans le manifeste de chaque tâche. Pour plus d'informations, consultez la page de CloudTrail tarification, qui contient des exemples illustrant la façon dont les prix changent en fonction du nombre de sentiers que vous avez configurés dans votre compte. Pour découvrir comment configurer et journaliser des événements en fonction de vos besoins, consultez Création de votre premier journal d'activité dans le Guide de l'utilisateur AWS CloudTrail .

Pour de plus amples informations sur les évènements Amazon S3, consultez Notifications d'événements Amazon S3.

Suivi de l'échec d'une tâche

Si une tâche d'opérations par lot S3 rencontre un problème qui l'empêche de s'exécuter avec succès, comme le fait de ne pas pouvoir lire le manifeste spécifié, elle échoue. Lorsqu'une tâche échoue, elle génère un ou plusieurs codes d'échec ou causes d'échec. La fonctionnalité d'opérations par lot S3 stocke les codes et les causes d'échec avec la tâche afin que vous puissiez les consulter en demandant les détails de la tâche. Si vous avez demandé un rapport de fin de tâche, ce dernier inclut également les codes et les raisons d'échec.

Pour empêcher les tâches d'exécuter un grand nombre d'opérations infructueuses, Amazon S3 impose un seuil d'échec à chaque tâche d'opérations par lot. Lorsqu'une tâche a exécuté au moins 1 000 tâches, Amazon S3 surveille le taux d'échec. Si, à un moment donné, le taux d'échec (le nombre de tâches ayant échoué par rapport au nombre total de tâches exécutées) dépasse 50 %, la tâche échoue. Lorsqu'une tâche échoue parce qu'elle dépasse ce seul, vous pouvez identifier la cause de cet échec. Il se peut, par exemple, que vous ayez inclus par erreur des objets dans le manifeste qui ne sont pas dans le compartiment spécifié. Après avoir corrigé les erreurs, vous pouvez renvoyer la tâche.

> **Note**
>
> La fonctionnalité d'opérations par lot S3 fonctionne de manière asynchrone et n'exécute pas nécessairement les tâches dans l'ordre d'apparition des objets dans le manifeste. Dès lors, vous ne pouvez pas utiliser l'ordre du manifeste pour déterminer les tâches d'objets qui réussissent et celles qui échouent. Vous pouvez plutôt examiner le rapport d'achèvement de la tâche (si vous en avez demandé un) ou consulter vos journaux d' AWS CloudTrail événements pour déterminer la source des échecs.

Rapports de fin de tâche

Lorsque vous créez une tâche, vous pouvez demander un rapport de fin de tâche. Si la fonctionnalité d'opérations par lot S3 invoque avec succès au moins une tâche, Amazon S3 génère un rapport de fin de tâche après avoir terminé l'exécution des tâches, après avoir échoué ou après avoir été annulé. Vous pouvez configurer le rapport de fin de tâche pour y inclure toutes les tâches ou uniquement celles ayant échoué.

Le rapport de fin de tâche inclut la configuration et le statut des tâches, ainsi que des informations sur chaque tâche, y compris la clé d'objet et la version, le statut, les codes d'erreur et la description

des erreurs. Les rapports de fin de tâche fournissent un moyen facile de consulter les résultats de vos tâches dans un format consolidé sans nécessiter de configuration supplémentaire. Les rapports de fin de tâche sont chiffrés à l'aide du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Pour obtenir un exemple de rapport de fin de tâche, consultez Exemples : Rapports de fin de tâche d'opérations par lot S3.

Si vous ne configurez pas de rapport d'achèvement, vous pouvez toujours surveiller et auditer votre tâche et ses tâches à l'aide d' CloudTrail Amazon CloudWatch. Pour plus d'informations, consultez les rubriques suivantes :

Rubriques

- Exemples : suivi d'une tâche S3 Batch Operations sur Amazon EventBridge via AWS CloudTrail
- Exemples : Rapports de fin de tâche d'opérations par lot S3

Exemples : suivi d'une tâche S3 Batch Operations sur Amazon EventBridge via AWS CloudTrail

L'activité de la tâche d'opérations par lot Amazon S3 est enregistrée en tant qu'événements dans AWS CloudTrail. Vous pouvez créer une règle personnalisée dans Amazon EventBridge et envoyer ces événements à la ressource de notification cible de votre choix, telle qu'Amazon Simple Notification Service (Amazon SNS).

> **Note**
>
> Amazon EventBridge est le moyen préféré pour gérer vos événements. Amazon CloudWatch Events est le même service sous-jacent et la même API, mais EventBridge ils EventBridge fournissent davantage de fonctionnalités. Les modifications que vous apportez dans l'une CloudWatch ou l'autre console ou qui EventBridge apparaissent dans chaque console. Pour plus d'informations, consultez le guide de EventBridge l'utilisateur Amazon.

Exemples de suivi

- Événements S3 Batch Operations enregistrés dans CloudTrail
- EventBridge règle de suivi des événements liés aux tâches S3 Batch Operations

Événements S3 Batch Operations enregistrés dans CloudTrail

Lorsqu'une tâche Batch Operations est créée, elle est enregistrée en tant qu'`JobCreated`événement dans CloudTrail. Au fur et à mesure que la tâche s'exécute, elle change d'état pendant le traitement et d'autres `JobStatusChanged` événements sont enregistrés dans CloudTrail. Vous pouvez afficher ces événements sur la consoleCloudTrail . Pour plus d'informations CloudTrail, consultez le guide de AWS CloudTrail l'utilisateur.

> **Note**
>
> Seuls les `status-change` événements du job S3 Batch Operations sont enregistrés dans CloudTrail.

Example — Événement d'achèvement de la tâche S3 Batch Operations enregistré par CloudTrail

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-05T18:25:30Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f907577b-bf3d-4c53-b9ed-8a83a118a554",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "123412341234",
    "serviceEventDetails": {
        "jobId": "d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "jobArn": "arn:aws:s3:us-west-2:181572960644:job/
d6e58ec4-897a-4b6d-975f-10d7f0fb63ce",
        "status": "Complete",
        "jobEventId": "b268784cf0a66749f1a05bce259804f5",
        "failureCodes": [],
        "statusChangeReason": []
    }
```

```
}
```

EventBridge règle de suivi des événements liés aux tâches S3 Batch Operations

L'exemple suivant montre comment créer une règle dans Amazon EventBridge pour capturer les événements S3 Batch Operations enregistrés par AWS CloudTrail une cible de votre choix.

Pour ce faire, vous devez créer une règle en suivant toutes les étapes de la section Création de EventBridge règles réagissant aux événements. Vous collez la stratégie de modèle d'événement personnalisé d'opérations par lot S3 suivante, le cas échéant, et vous choisissez le service cible de votre choix.

Stratégie de modèle d'événement personnalisé d'opérations par lots S3

```
{
    "source": [
        "aws.s3"
    ],
    "detail-type": [
        "AWS Service Event via CloudTrail"
    ],
    "detail": {
        "eventSource": [
            "s3.amazonaws.com"
        ],
        "eventName": [
            "JobCreated",
            "JobStatusChanged"
        ]
    }
}
```

Les exemples suivants présentent deux événements Batch Operations envoyés à Amazon Simple Queue Service (Amazon SQS) à partir EventBridge d'une règle d'événement. Une tâche d'opérations par lot passe par de nombreux états différents pendant son traitement (`New`, `Preparing`, `Active`, etc.), de sorte que vous pouvez vous attendre à recevoir plusieurs messages pour chaque tâche.

Example - Exemple d'événement JobCreated

```
{
    "version": "0",
```

```
    "id": "51dc8145-541c-5518-2349-56d7dffdf2d8",
    "detail-type": "AWS Service Event via CloudTrail",
    "source": "aws.s3",
    "account": "123456789012",
    "time": "2020-02-27T15:25:49Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventVersion": "1.05",
        "userIdentity": {
            "accountId": "11112223334444",
            "invokedBy": "s3.amazonaws.com"
        },
        "eventTime": "2020-02-27T15:25:49Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "JobCreated",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "s3.amazonaws.com",
        "userAgent": "s3.amazonaws.com",
        "eventID": "7c38220f-f80b-4239-8b78-2ed867b7d3fa",
        "readOnly": false,
        "eventType": "AwsServiceEvent",
        "serviceEventDetails": {
            "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
            "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
            "status": "New",
            "jobEventId": "f177ff24f1f097b69768e327038f30ac",
            "failureCodes": [],
            "statusChangeReason": []
        }
    }
}
```

Example — Événement de fin de tâche JobStatusChanged

```
{
  "version": "0",
  "id": "c8791abf-2af8-c754-0435-fd869ce25233",
  "detail-type": "AWS Service Event via CloudTrail",
  "source": "aws.s3",
  "account": "123456789012",
  "time": "2020-02-27T15:26:42Z",
```

```
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "eventVersion": "1.05",
    "userIdentity": {
      "accountId": "1111222233334444",
      "invokedBy": "s3.amazonaws.com"
    },
    "eventTime": "2020-02-27T15:26:42Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "JobStatusChanged",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "s3.amazonaws.com",
    "userAgent": "s3.amazonaws.com",
    "eventID": "0238c1f7-c2b0-440b-8dbd-1ed5e5833afb",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "serviceEventDetails": {
      "jobId": "e849b567-5232-44be-9a0c-40988f14e80c",
      "jobArn": "arn:aws:s3:us-east-1:181572960644:job/
e849b567-5232-44be-9a0c-40988f14e80c",
      "status": "Complete",
      "jobEventId": "51f5ac17dba408301d56cd1b2c8d1e9e",
      "failureCodes": [],
      "statusChangeReason": []
    }
  }
}
```


Exemples : Rapports de fin de tâche d'opérations par lot S3

Lorsque vous créez une tâche d'opérations par lot S3, vous pouvez demander un rapport de fin de tâche pour toutes les tâches ou uniquement pour les tâches qui ont échoué. Tant qu'au moins une tâche a été invoquée avec succès, la fonctionnalité d'opérations par lot S3 génère un rapport pour les tâches qui ont été achevées, qui ont échoué ou qui ont été annulées.

Le rapport de fin contient des informations complémentaires pour chaque tâche, y compris le nom et la version des clés d'objets, le statut, les codes d'erreurs et les descriptions des erreurs éventuelles. La description des erreurs pour chaque tâche ayant échoué peut être utilisée pour diagnostiquer les problèmes pendant la création de tâches, par exemple les autorisations.

> **Note**
>
> Les rapports de fin de tâche sont toujours chiffrés avec des clés gérées par Amazon S3 (SSE-S3).

Example - Fichier de résultats de manifeste de niveau supérieur

Le fichier `manifest.json` de niveau supérieur contient les emplacements de chaque rapport réussi et (si la tâche a présenté des échecs) l'emplacement des rapports ayant échoué, comme montré dans l'exemple suivant.

```
{
    "Format": "Report_CSV_20180820",
    "ReportCreationDate": "2019-04-05T17:48:39.725Z",
    "Results": [
        {
            "TaskExecutionStatus": "succeeded",
            "Bucket": "my-job-reports",
            "MD5Checksum": "83b1c4cbe93fc893f54053697e10fd6e",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/
results/6217b0fab0de85c408b4be96aeaca9b195a7daa5.csv"
        },
        {
            "TaskExecutionStatus": "failed",
            "Bucket": "my-job-reports",
            "MD5Checksum": "22ee037f3515975f7719699e5c416eaa",
            "Key": "job-f8fb9d89-a3aa-461d-bddc-ea6a1b131955/results/
b2ddad417e94331e9f37b44f1faf8c7ed5873f2e.csv"
        }
    ],
    "ReportSchema": "Bucket, Key, VersionId, TaskStatus, ErrorCode, HTTPStatusCode,
 ResultMessage"
}
```

Example - Rapports des tâches ayant échoué

Les rapports des tâches ayant échoué contiennent les informations suivantes pour toutes les tâches ayant échoué :

- `Bucket`

- `Key`
- `VersionId`
- `TaskStatus`
- `ErrorCode`
- `HTTPStatusCode`
- `ResultMessage`

L'exemple de rapport suivant montre un cas dans lequel la AWS Lambda fonction a expiré, entraînant des défaillances dépassant le seuil de défaillance. La mention `PermanentFailure` a alors été apposée.

```
amzn-s3-demo-bucket1,image_14975,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:21.155Z 2845ca0d-38d9-4c4b-
abcf-379dc749c452 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15897,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.610Z 2d0a330b-de9b-425f-
b511-29232fde5fe4 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_14819,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:22.362Z fcf5efde-74d4-4e6d-b37a-
c7f18827f551 Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_15930,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:29.809Z 3dd5b57c-4a4a-48aa-8a35-
cbf027b7957e Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17644,,failed,200,PermanentFailure,"Lambda
 returned function error: {""errorMessage"":""2019-04-05T17:35:46.025Z
 10a764e4-2b26-4d8c-9056-1e1072b4723f Task timed out after 3.00 seconds""}"
amzn-s3-demo-bucket1,image_17398,,failed,200,PermanentFailure,"Lambda returned
 function error: {""errorMessage"":""2019-04-05T17:35:44.661Z 1e306352-4c54-4eba-
aee8-4d02f8c0235c Task timed out after 3.00 seconds""}"
```

Example - Rapport des tâches réussies

Les rapports des tâches réussies contiennent les éléments suivants pour toutes les tâches réussies :

- `Bucket`
- `Key`
- `VersionId`
- `TaskStatus`

- `ErrorCode`
- `HTTPStatusCode`
- `ResultMessage`

Dans l'exemple suivant, la fonction Lambda a copié avec succès l'objet Amazon S3 dans un autre compartiment. La réponse Amazon S3 retournée est renvoyée à la fonctionnalité d'opérations par lot S3 et est ensuite écrite dans le rapport d'achèvement final.

```
amzn-s3-demo-bucket1,image_17775,,succeeded,200,,"{u'CopySourceVersionId':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'RequestId': '3ED5852152014362', 'HTTPHeaders':
 {'content-length': '234', 'x-amz-id-2': 'nXNaClIMxEJzWNmeMNQV2KpjbaCJLn0OGoXWZpuVOFS/
iQYWxb3QtTvzX9SVfx2lA3oTKLwImKw=', 'x-amz-copy-source-version-id':
 'xVR78haVKlRnurYofbTfYr3ufYbktF8h', 'server': 'AmazonS3', 'x-amz-request-id':
 '3ED5852152014362', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT', 'content-type':
 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17763,,succeeded,200,,"{u'CopySourceVersionId':
 '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 39, tzinfo=tzlocal()),
 u'ETag': '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata':
 {'HTTPStatusCode': 200, 'RetryAttempts': 0, 'HostId': 'GiCZNYr8LHd/
Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'RequestId':
 '1BC9F5B1B95D7000', 'HTTPHeaders': {'content-length': '234', 'x-amz-id-2':
 'GiCZNYr8LHd/Thyk6beTRP96IGZk2sYxujLe13TuuLpq6U2RD3we0YoluuIdm1PRvkMwnEW1aFc=', 'x-
amz-copy-source-version-id': '6HjOUSim4Wj6BTcbxToXW44pSZ.40pwq', 'server': 'AmazonS3',
 'x-amz-request-id': '1BC9F5B1B95D7000', 'date': 'Fri, 05 Apr 2019 17:35:39 GMT',
 'content-type': 'application/xml'}}}"
amzn-s3-demo-bucket1,image_17860,,succeeded,200,,"{u'CopySourceVersionId':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', u'CopyObjectResult': {u'LastModified':
 datetime.datetime(2019, 4, 5, 17, 35, 40, tzinfo=tzlocal()), u'ETag':
 '""fe66f4390c50f29798f040d7aae72784""'}, 'ResponseMetadata': {'HTTPStatusCode':
 200, 'RetryAttempts': 0, 'HostId': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'RequestId': '8D9CA56A56813DF3', 'HTTPHeaders':
 {'content-length': '234', 'x-amz-id-2': 'F9ooZOgpE5g9sNgBZxjdiPHqB4+0DNWgj3qbsir
+sKai4fv7rQEcF2fBN1VeeFc2WH45a9ygb2g=', 'x-amz-copy-source-version-id':
 'm.MDD0g_QsUnYZ8TBzVFrp.TmjN8PJyX', 'server': 'AmazonS3', 'x-amz-request-id':
 '8D9CA56A56813DF3', 'date': 'Fri, 05 Apr 2019 17:35:40 GMT', 'content-type':
 'application/xml'}}}"
```

Contrôle de l'accès et étiquetage des tâches à l'aide d'étiquettes

Vous pouvez étiqueter et contrôler l'accès à vos tâches d'opérations par lot S3 en ajoutant des étiquettes. Les étiquettes peuvent être utilisées pour identifier la personne qui est responsable d'une tâche d'opérations par lot. La présence d'étiquettes de tâche peut octroyer ou limiter la capacité d'un utilisateur à annuler une tâche, activer une tâche dans l'état de confirmation ou modifier le niveau de priorité d'une tâche. Vous pouvez créer des tâches avec des balises qui leur sont attachées et ajouter des balises aux tâches une fois qu'elles ont été créées. Chaque étiquette est une paire clé-valeur que vous pouvez ajouter lors de la création de la tâche ou de sa mise à jour ultérieure.

> **Warning**
>
> Assurez-vous que les balises de tâche ne contiennent aucune information confidentielle ni donnée personnelle.

Prenons l'exemple d'étiquetage suivant : supposons que vous souhaitez que votre service Finance crée une tâche d'opérations par lot. Vous pouvez écrire une politique AWS Identity and Access Management (IAM) qui permet à un utilisateur d'appeler`CreateJob`, à condition que la tâche soit créée avec la valeur `Finance` attribuée à la `Department` balise. En outre, vous pouvez attacher cette stratégie à tous les utilisateurs qui sont membres du département des finances.

En continuant avec cet exemple, vous pouvez écrire une stratégie qui permet à un utilisateur de mettre à jour la priorité de n'importe quelle tâche comportant les étiquettes souhaitées, ou d'annuler toute tâche qui les possède. Pour de plus amples informations, veuillez consulter the section called "Contrôle des autorisations".

Vous pouvez ajouter des identifications à de nouvelles tâches d'opérations par lot S3 lors de leur création ou les ajouter aux tâches existantes.

Notez les restrictions suivantes liées aux étiquettes :

- Vous pouvez associer jusqu'à 50 étiquettes à une tâche, à condition qu'elles aient des clés d'étiquette uniques.
- Une clé d'étiquette peut comporter jusqu'à 128 caractères Unicode et les valeurs d'étiquette peuvent comporter jusqu'à 256 caractères Unicode.
- La clé et les valeurs sont sensibles à la casse.

Pour de plus amples informations sur les restrictions liées aux étiquettes, consultez Restrictions encadrant les étiquettes définies par l'utilisateur dans le Guide de l'utilisateur AWS Billing and Cost Management .

Opérations d'API liées au balisage des tâches d'opérations par lot S3

Amazon S3 prend en charge les opérations d'API suivantes qui sont spécifiques au balisage des tâches d'opérations par lot S3 :

- GetJobTagging – renvoie l'ensemble de balises associé à une tâche d'opérations par lot.
- PutJobTagging – Remplace l'ensemble de balises associé à une tâche. Il existe deux scénarios de gestion d'étiquettes de tâches d'opérations par lot S3 à l'aide de cette API.
  - La tâche n'a pas de balise : vous pouvez ajouter un ensemble de balises à une tâche (la tâche n'a pas de balises antérieures).
  - La tâche a un ensemble de balises : pour modifier cet ensemble de balises, vous pouvez soit le remplacer entièrement, soit y apporter des modifications en extrayant l'ensemble de balises à l'aide de GetJobTagging, en apportant les modifications nécessaires et en utilisant cette action d'API pour remplacer l'ensemble de balises par celui que vous avez modifié.

    > **Note**
    >
    > Si vous envoyez cette demande avec un ensemble d'étiquettes vide, la fonctionnalité d'opérations par lot S3 supprime l'ensemble d'étiquettes existant de l'objet. Si vous employez cette méthode, une demande de Niveau 1 (PUT) vous est facturée. Pour de plus amples informations, veuillez consulter Tarification Amazon S3.
    > Pour supprimer des étiquettes existantes pour votre tâche d'opérations par lot, l'action `DeleteJobTagging` est préférable, car elle permet d'obtenir le même résultat sans frais.

- DeleteJobTagging – Supprime l'ensemble de balises associé à une tâche d'opérations par lot.

Création d'une tâche d'opérations par lot avec des étiquettes de tâche utilisées pour l'étiquetage

Vous pouvez étiqueter et contrôler l'accès à vos tâches d'opérations par lot Amazon S3 en ajoutant des balises. Les étiquettes peuvent être utilisées pour identifier la personne qui est responsable d'une tâche d'opérations par lot. Vous pouvez créer des tâches avec des étiquettes qui leur sont

attachées et ajouter des étiquettes aux tâches une fois qu'elles ont été créées. Pour de plus amples informations, veuillez consulter the section called "Utilisation d'étiquettes".

À l'aide du AWS CLI

L' AWS CLI exemple suivant crée une `S3PutObjectCopy` tâche S3 Batch Operations en utilisant des balises de tâche comme étiquettes pour la tâche.

1. Sélectionnez l'action ou `OPERATION` que la tâche d'opérations par lot doit exécuter et choisissez votre élément `TargetResource`.

```
read -d '' OPERATION <<EOF
{
  "S3PutObjectCopy": {
    "TargetResource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
  }
}
EOF
```

2. Identifiez les `TAGS` de tâche que vous voulez pour la tâche. Dans ce cas, vous appliquez deux étiquettes, `department` et `FiscalYear`, avec les valeurs `Marketing` et `2020` respectivement.

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

3. Spécifiez l'élément `MANIFEST` pour la tâche d'opérations par lot.

```
read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "EXAMPLE_S3BatchOperations_CSV_20180820",
    "Fields": [
```

```
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/example_manifest.csv",
    "ETag": "example-5dc7a8bfb90808fc5d546218"
  }
}
EOF
```

4. Configurez l'élément REPORT pour la tâche d'opérations par lot.

```
read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Example_Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/copy-with-replace-metadata",
  "ReportScope": "AllTasks"
}
EOF
```

5. Exécutez l'action `create-job` pour créer votre tâche d'opérations par lot avec les entrées définies dans les étapes précédentes.

```
aws \
    s3control create-job \
    --account-id 123456789012 \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn arn:aws:iam::123456789012:role/batch-operations-role \
    --tags "${TAGS//$'\n'/}" \
    --client-request-token "$(uuidgen)" \
    --region us-west-2 \
    --description "Copy with Replace Metadata";
```

Utilisation du AWS SDK pour Java

Example

L'exemple suivant crée une tâche d'opérations par lot S3 avec des étiquettes à l'aide du kit AWS SDK pour Java.

```
public String createJob(final AWSS3ControlClient awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
manifests/10_manifest.csv";
    final String manifestObjectVersionId = "example-5dc7a8bfb90808fc5d546218";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new
 JobManifestSpec().withFormat(JobManifestFormat.S3InventoryReport_CSV_20161130);

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "example-job-reports";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final String lambdaFunctionArn = "arn:aws:lambda:us-
west-2:123456789012:function:example-function";

    final JobOperation jobOperation = new JobOperation()
            .withLambdaInvoke(new
 LambdaInvokeOperation().withFunctionArn(lambdaFunctionArn));

    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
```

```
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");

    final String roleArn = "arn:aws:iam::123456789012:role/example-batch-operations-
role";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Test lambda job")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withTags(departmentTag, fiscalYearTag)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Suppression des étiquettes d'une tâche d'opérations par lot S3

Vous pouvez utiliser ces exemples pour supprimer les balises d'une tâche d'opérations par lot Amazon S3.

À l'aide du AWS CLI

L'exemple suivant supprime les étiquettes d'une tâche d'opérations par lot à l'aide de la AWS CLI.

```
aws \
    s3control delete-job-tagging \
    --account-id 123456789012 \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

Supprimer les étiquettes d'une tâche d'opérations par lot

Example

L'exemple suivant supprime les étiquettes d'une tâche d'opérations par lot S3 à l'aide du kit AWS SDK pour Java.

```
public void deleteJobTagging(final AWSS3ControlClient awss3ControlClient,
                             final String jobId) {
    final DeleteJobTaggingRequest deleteJobTaggingRequest = new
 DeleteJobTaggingRequest()
            .withJobId(jobId);

    final DeleteJobTaggingResult deleteJobTaggingResult =
                awss3ControlClient.deleteJobTagging(deleteJobTaggingRequest);
}
```

Ajout de balises dans une tâche d'opérations par lot existante

Vous pouvez utiliser l'opération d'API PutJobTagging pour ajouter des balises à vos tâches d'opérations par lot Amazon S3 existantes. Pour plus d'informations, consultez les exemples suivants.

À l'aide du AWS CLI

Voici un exemple d'utilisation de `s3control put-job-tagging` pour ajouter des balises à une tâche d'opérations par lot S3 à l'aide de l' AWS CLI. Pour utiliser ces exemples, remplacez *`user input placeholders`* par vos propres informations.

> **Note**
>
> Si vous envoyez cette demande avec un ensemble de balises vide, la fonctionnalité d'opérations par lot supprime l'ensemble de balises existant de l'objet. Cependant, si vous utilisez cette méthode, une demande de Niveau 1 (PUT) vous est facturée. Pour plus d'informations, consultez Tarification Amazon S3.
>
> Au lieu de cela, pour supprimer des balises existantes pour votre tâche d'opérations par lot, nous vous recommandons d'utiliser l'opération `DeleteJobTagging`, car elle permet d'obtenir le même résultat sans frais.

1. Identifiez les TAGS de tâche que vous voulez pour la tâche. Dans ce cas, vous appliquez deux étiquettes, *department* et *FiscalYear*, avec les valeurs *Marketing* et *2020* respectivement.

```
read -d '' TAGS <<EOF
[
  {
    "Key": "department",
    "Value": "Marketing"
  },
  {
    "Key": "FiscalYear",
    "Value": "2020"
  }
]
EOF
```

2. Exécutez la commande `put-job-tagging` suivante avec les paramètres requis :

```
aws \
    s3control put-job-tagging \
    --account-id 123456789012 \
    --tags "${TAGS//$'\n'/}" \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

Utilisation du AWS SDK pour Java

Example

L'exemple suivant montre comment placer les balises d'une tâche d'opérations par lot S3 à l'aide du kit AWS SDK pour Java.

```
public void putJobTagging(final AWSS3ControlClient awss3ControlClient,
                          final String jobId) {
    final S3Tag departmentTag = new
 S3Tag().withKey("department").withValue("Marketing");
    final S3Tag fiscalYearTag = new S3Tag().withKey("FiscalYear").withValue("2020");

    final PutJobTaggingRequest putJobTaggingRequest = new PutJobTaggingRequest()
            .withJobId(jobId)
            .withTags(departmentTag, fiscalYearTag);
```

```
    final PutJobTaggingResult putJobTaggingResult =
 awss3ControlClient.putJobTagging(putJobTaggingRequest);
}
```

Obtention des étiquettes d'une tâche d'opérations par lot S3

Pour récupérer les balises d'une tâche d'opérations par lot Amazon S3, vous pouvez utiliser l'opération d'API `GetJobTagging`. Pour plus d'informations, consultez les exemples suivants.

À l'aide du AWS CLI

L'exemple suivant permet d'obtenir les étiquettes d'une tâche d'opérations par lot à l'aide de la AWS CLI. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws \
    s3control get-job-tagging \
    --account-id 123456789012 \
    --job-id Example-e25a-4ed2-8bee-7f8ed7fc2f1c \
    --region us-east-1
```

Utilisation du AWS SDK pour Java

Example

L'exemple suivant permet d'obtenir les étiquettes d'une tâche d'opérations par lot S3 à l'aide de la AWS SDK pour Java.

```
public List<S3Tag> getJobTagging(final AWSS3ControlClient awss3ControlClient,
                                 final String jobId) {
    final GetJobTaggingRequest getJobTaggingRequest = new GetJobTaggingRequest()
            .withJobId(jobId);

    final GetJobTaggingResult getJobTaggingResult =
            awss3ControlClient.getJobTagging(getJobTaggingRequest);

    final List<S3Tag> tags = getJobTaggingResult.getTags();

    return tags;
}
```

Contrôle des autorisations pour les opérations par lot à l'aide de balises de tâche

Pour faciliter la gestion des tâches d'opérations par lot Amazon S3, vous pouvez ajouter des balises de tâche. Les étiquettes de tâche vous permettent de contrôler l'accès à vos tâches d'opérations par lot et d'imposer l'application d'étiquettes lors de la création de toute tâche.

Vous pouvez appliquer jusqu'à 50 étiquettes de tâche à chaque tâche d'opérations par lot. L'utilisation de balises vous permet de définir des politiques granulaires limitant l'ensemble d'utilisateurs qui peuvent modifier la tâche. Les étiquettes de tâche peuvent octroyer ou limiter la capacité d'un utilisateur à annuler une tâche, activer une tâche dans l'état de confirmation ou modifier le niveau de priorité d'une tâche. En outre, vous pouvez exiger l'application d'étiquettes à toutes les nouvelles tâches et spécifier les paires clé-valeur autorisées pour les étiquettes. Vous pouvez exprimer toutes ces conditions en utilisant le même langage de politique AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

L'exemple suivant montre comment utiliser des étiquettes de tâche d'opérations par lot S3 pour accorder aux utilisateurs l'autorisation de créer et de modifier uniquement les tâches exécutées au sein d'un service spécifique (par exemple, le service Finance ou Conformité). Vous pouvez également affecter des tâches en fonction du stade de développement auquel elles sont liées, notamment l'assurance qualité ou la production.

Dans cet exemple, vous utilisez les balises de la tâche d'opérations par lot S3 dans les politique IAM pour accorder aux utilisateurs l'autorisation de créer et de modifier uniquement les tâches exécutées au sein de leur service. Vous affectez des tâches en fonction du stade de développement auquel elles sont liées, telles que l'assurance qualité ou la production.

Les exemples suivants utilisent les services suivants, chacun utilisant les tâches d'opérations par lot de différentes manières :

- Finance
- Conformité
- Business Intelligence
- Ingénierie

Rubriques

- Contrôler l'accès en affectant des étiquettes aux utilisateurs et aux ressources
- Balisage des tâches d'opérations par lot par étape et application de limites sur la priorité des tâches

Contrôler l'accès en affectant des étiquettes aux utilisateurs et aux ressources

Dans ce scénario, les administrateurs utilisent le contrôle d'accès basé sur les attributs (ABAC). ABAC est une stratégie d'autorisation IAM qui définit les autorisations en attachant des balises aux utilisateurs et AWS aux ressources.

Les utilisateurs et les tâches se voient attribuer l'une des étiquettes de service suivantes :

Clé : Valeur

- `department : Finance`
- `department : Compliance`
- `department : BusinessIntelligence`
- `department : Engineering`

> **Note**
>
> Les clés et valeurs d'étiquette sont sensibles à la casse.

À l'aide de la stratégie de contrôle d'accès ABAC, vous accordez à un utilisateur du service Finance l'autorisation de créer et de gérer des tâches d'opérations par lot S3 au sein de son service en associant l'étiquette `department=Finance` à son utilisateur.

En outre, vous pouvez attacher à l'utilisateur IAM une stratégie gérée qui permet à tout utilisateur de son entreprise de créer ou de modifier des tâches d'opérations par lot S3 au sein des différents services.

La stratégie de cet exemple comprend trois déclarations de stratégie :

- La première déclaration de la stratégie permet à l'utilisateur de créer une tâche d'opérations par lot à condition que la demande de création de tâche comprenne une étiquette de tâche correspondant à son service. Ceci est exprimé à l'aide de la syntaxe `"${aws:PrincipalTag/department}"`, qui est remplacée par l'étiquette du service de l'utilisateur au moment de l'évaluation de la

stratégie. La condition est remplie lorsque la valeur fournie pour l'étiquette du service dans la demande (`"aws:RequestTag/department"`) correspond au département de l'utilisateur.

- La deuxième déclaration de la stratégie permet aux utilisateurs de modifier la priorité des tâches ou de mettre à jour le statut d'une tâche, à condition que la tâche mise à jour corresponde au service de l'utilisateur.
- La troisième déclaration permet à un utilisateur de mettre à jour les étiquettes d'une tâche d'opérations par lot à tout moment via une demande `PutJobTagging`, à condition que (1) l'étiquette de son service soit conservée et (2) la tâche qu'il met à jour se trouve dans son département.

JSON

```
{
      "Version": "2012-10-17",
      "Statement": [
            {
                  "Effect": "Allow",
                  "Action": "s3:CreateJob",
                  "Resource": "*",
                  "Condition": {
                        "StringEquals": {
                              "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
            {
                  "Effect": "Allow",
                  "Action": [
                        "s3:UpdateJobPriority",
                        "s3:UpdateJobStatus"
            ],
                  "Resource": "*",
                  "Condition": {
                        "StringEquals": {
                              "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
```

```
            {
                  "Effect": "Allow",
                  "Action": "s3:PutJobTagging",
                  "Resource": "*",
                  "Condition": {
                        "StringEquals": {
                              "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                              "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                  }
            }
        }
    ]
}
```

Balisage des tâches d'opérations par lot par étape et application de limites sur la priorité des tâches

Toutes les tâches d'opérations par lot S3 ont une priorité numérique, qu'Amazon S3 utilise pour décider de leur ordre d'exécution. Dans cet exemple, vous limitez la priorité maximale que la plupart des utilisateurs peuvent affecter aux tâches, avec des plages de priorité plus élevées réservées à un ensemble limité d'utilisateurs privilégiés, comme suit :

- Plage de priorité de l'étape assurance qualité (faible) : 1-100
- Plage de priorité de l'étape production (élevée) : 1-300

Pour ce faire, introduisez un nouveau jeu d'étiquettes représentant l'étape de la tâche :

Clé : Valeur

- `stage : QA`
- `stage : Production`

Création et mise à jour de tâches à faible priorité au sein d'un service

Cette stratégie introduit deux nouvelles restrictions sur la création et la mise à jour de tâches d'opérations par lot S3, en plus de la restriction basée sur le service :

- Les utilisateurs peuvent créer ou mettre à jour des tâches dans leur service avec une nouvelle condition qui exige que la tâche inclue l'étiquette `stage=QA`.
- Les utilisateurs peuvent créer ou mettre à jour la priorité d'une tâche jusqu'à une nouvelle priorité maximale de 100.

```
{
        "Version": "2012-10-17",
        "Statement": [
        {
        "Effect": "Allow",
        "Action": "s3:CreateJob",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA"
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:UpdateJobStatus"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:UpdateJobPriority",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:ResourceTag/stage": "QA"
```

```
            },
            "NumericLessThanEquals": {
                "s3:RequestJobPriority": 100
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:PutJobTagging",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/department" : "${aws:PrincipalTag/department}",
                "aws:ResourceTag/department": "${aws:PrincipalTag/department}",
                "aws:RequestTag/stage": "QA",
                "aws:ResourceTag/stage": "QA"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "s3:GetJobTagging",
        "Resource": "*"
    }
    ]
}
```

Création et mise à jour de tâches hautement prioritaires au sein d'un service

Un petit nombre d'utilisateurs peut avoir besoin de créer des tâches hautement prioritaires dans les services de l'assurance qualité ou de la production. Pour répondre à ce besoin, vous créez une stratégie gérée adaptée à la stratégie de faible priorité décrite dans la section précédente.

Cette stratégie effectue les opérations suivantes :

- Elle permet aux utilisateurs de créer ou de mettre à jour des tâches dans leur service avec l'étiquette `stage=QA` ou `stage=Production`.
- Elle permet aux utilisateurs de créer ou de mettre à jour la priorité d'une tâche jusqu'à un maximum de 300.

JSON

```
{
      "Version": "2012-10-17",
      "Statement": [
          {
                "Effect": "Allow",
                "Action": "s3:CreateJob",
                "Resource": "*",
                "Condition": {
                      "ForAnyValue:StringEquals": {
                            "aws:RequestTag/stage": [
                                  "QA",
                                  "Production"
                    ]
                },
                      "StringEquals": {
                            "aws:RequestTag/department": "${aws:PrincipalTag/
department}"
                },
                      "NumericLessThanEquals": {
                            "s3:RequestJobPriority": 300
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": [
                      "s3:UpdateJobStatus"
            ],
                "Resource": "*",
                "Condition": {
                      "StringEquals": {
                            "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:UpdateJobPriority",
                "Resource": "*",
                "Condition": {
```

```
                    "ForAnyValue:StringEquals": {
                        "aws:ResourceTag/stage": [
                            "QA",
                            "Production"
                    ]
                },
                    "StringEquals": {
                        "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                    "NumericLessThanEquals": {
                        "s3:RequestJobPriority": 300
                }
            }
        },
          {
                "Effect": "Allow",
                "Action": "s3:PutJobTagging",
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "aws:RequestTag/department": "${aws:PrincipalTag/
department}",
                        "aws:ResourceTag/department": "${aws:PrincipalTag/
department}"
                },
                    "ForAnyValue:StringEquals": {
                        "aws:RequestTag/stage": [
                            "QA",
                            "Production"
                    ],
                        "aws:ResourceTag/stage": [
                            "QA",
                            "Production"
                    ]
                }
            }
        }
    ]
}
```

Gestion du verrouillage des objets S3 à l'aide des opérations par lot S3

Vous pouvez utiliser les opérations par lot S3 pour effectuer des opérations par lot à grande échelle sur des objets Amazon S3. Les opérations par lot S3 peuvent effectuer une seule opération sur les listes d'objets Amazon S3 que vous spécifiez. Une seule tâche peut effectuer une opération spécifiée sur des milliards d'objets contenant des exaoctets de données. Amazon S3 suit la progression, envoie des notifications et stocke un rapport de fin d'opérations détaillé sur toutes les actions, offrant ainsi une expérience sans serveur entièrement gérée et contrôlable. Vous pouvez utiliser S3 Batch Operations via la console Amazon S3 ou AWS SDKs l'API REST Amazon S3. AWS CLI

Avec le verrouillage d'objets S3, vous pouvez aussi mettre en place une conservation légale sur une version d'objet. À l'instar d'une période de rétention, une conservation légale empêche une version d'objet d'être remplacée ou supprimée. Cependant, une conservation légale n'est associée à aucune période de rétention et reste en vigueur jusqu'à sa suppression. Pour de plus amples informations, veuillez consulter Mise en suspens juridique du verrouillage des objets S3.

Pour utiliser les opérations par lot S3 avec le verrouillage d'objet pour attribuer des conservations légales à plusieurs objets Amazon S3 à la fois, consultez les rubriques suivantes.

Rubriques

- Activation du verrouillage des objets S3 à l'aide des opérations par lot S3
- Définition de la rétention du verrouillage des objets à l'aide des opérations par lot
- Utilisation de la fonctionnalité d'opérations par lot S3 avec le mode de conformité de rétention du verrouillage des objets S3
- Utiliser la fonctionnalité d'opérations par lot S3 avec le mode de gouvernance de rétention du verrouillage des objets S3
- Utilisation de la fonctionnalité d'opérations par lot S3 pour désactiver la conservation légale du verrouillage d'objet S3

Activation du verrouillage des objets S3 à l'aide des opérations par lot S3

Vous pouvez utiliser la fonctionnalité d'opérations par lot Amazon S3 avec le verrouillage d'objet S3 pour gérer la rétention ou activer la conservation légale de nombreux objets Amazon S3 à la fois. Vous spécifiez la liste des objets cibles dans votre manifeste et l'envoyez aux tâches d'opérations par lot pour terminer. Pour plus d'informations, consultez the section called "Rétention du verrouillage d'objet" et the section called "Conservation légale du verrouillage d'objet".

Les exemples suivants montrent comment créer un rôle AWS Identity and Access Management (IAM) avec des autorisations S3 Batch Operations et comment mettre à jour les autorisations de rôle pour créer des tâches qui activent Object Lock. Vous devez également disposer d'un manifeste CSV qui identifie les objets de votre tâche d'opérations par lot S3. Pour de plus amples informations, veuillez consulter the section called "Spécification d'un manifeste".

Pour utiliser les exemples suivants, remplacez *user input placeholders* par vos propres informations.

À l'aide du AWS CLI

1. Créez un rôle IAM et autorisez les tâches d'opérations par lot S3 à s'exécuter.

   Cette étape est obligatoire pour toutes les tâches d'opérations par lot S3.

   ```
   export AWS_PROFILE='aws-user'

   read -d '' batch_operations_trust_policy <<EOF
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Effect": "Allow",
         "Principal": {
           "Service": [
             "batchoperations.s3.amazonaws.com"
           ]
         },
         "Action": "sts:AssumeRole"
       }
     ]
   }
   EOF
   aws iam create-role --role-name batch_operations-objectlock \
   --assume-role-policy-document "${batch_operations_trust_policy}"
   ```

2. Configurez l'exécution des tâches d'opérations par lot S3 avec la fonctionnalité de verrouillage des objets S3.

   Dans cette étape, vous autorisez le rôle à effectuer les opérations suivantes :

a. Exécutez la tâche de verrouillage des objets sur le compartiment S3 qui contient les objets cibles sur lesquels vous souhaitez exécuter la fonctionnalité d'opérations par lot.

b. Lisez le compartiment S3 où se trouvent le fichier CSV manifeste et les objets.

c. Écrivez les résultats de la tâche d'opérations par lot S3 dans le compartiment de rapports.

```
read -d '' batch_operations_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "s3:GetBucketObjectLockConfiguration",
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetBucketLocation"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-completion-report-bucket}}/*"
            ]
        }
    ]
}
EOF
```

```
aws iam put-role-policy --role-name batch_operations-objectlock \
--policy-name object-lock-permissions \
--policy-document "${batch_operations_permissions}"
```

Utilisation du AWS SDK pour Java

Les exemples suivants montrent comment créer un rôle IAM avec des autorisations d'opérations par lot S3 et comment mettre à jour les autorisations de rôle pour créer des tâches qui activent le verrouillage d'objet à l'aide du kit AWS SDK pour Java. Vous devez également disposer d'un manifeste CSV identifiant les objets de votre tâche d'opérations par lot S3. Pour de plus amples informations, veuillez consulter the section called "Spécification d'un manifeste".

Procédez comme suit :

1. Créez un rôle IAM et autorisez les tâches d'opérations par lot S3 à s'exécuter. Cette étape est obligatoire pour toutes les tâches d'opérations par lot S3.
2. Configurez l'exécution des tâches d'opérations par lot S3 avec la fonctionnalité de verrouillage des objets S3.

   Vous autorisez le rôle à effectuer les opérations suivantes :

   1. Exécutez la tâche de verrouillage des objets sur le compartiment S3 qui contient les objets cibles sur lesquels vous souhaitez exécuter la fonctionnalité d'opérations par lot.
   2. Lisez le compartiment S3 où se trouvent le fichier CSV manifeste et les objets.
   3. Écrivez les résultats de la tâche d'opérations par lot S3 dans le compartiment de rapports.

```
public void createObjectLockRole() {
    final String roleName = "batch_operations-object-lock";

    final String trustPolicy = "{" +
            "  \"Version\": \"2012-10-17\", " +
            "  \"Statement\": [ " +
            "    { " +
            "      \"Effect\": \"Allow\", " +
            "      \"Principal\": { " +
            "        \"Service\": [" +
            "          \"batchoperations.s3.amazonaws.com\"" +
            "        ]" +
            "      }, " +
```

```
            "      \"Action\": \"sts:AssumeRole\" " +
            "    } " +
            "  ]" +
            "}";

    final String bopsPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": \"s3:GetBucketObjectLockConfiguration\"," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket\"" +
            "            ]" +
            "        }," +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:GetObject\"," +
            "                \"s3:GetObjectVersion\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }," +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObject\"," +
            "                \"s3:GetBucketLocation\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*\""
+
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final CreateRoleRequest createRoleRequest = new CreateRoleRequest()
```

```
            .withAssumeRolePolicyDocument(bopsPermissions)
            .withRoleName(roleName);

    final CreateRoleResult createRoleResult = iam.createRole(createRoleRequest);

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bopsPermissions)
            .withPolicyName("batch_operations-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

Définition de la rétention du verrouillage des objets à l'aide des opérations par lot

Vous pouvez utiliser les opérations par lot Amazon S3 avec le verrouillage d'objet S3 pour gérer la conservation de nombreux objets Amazon S3 à la fois. Vous spécifiez la liste des objets cibles dans votre manifeste et l'envoyez aux tâches d'opérations par lot pour terminer. Pour plus d'informations, consultez the section called "Rétention du verrouillage d'objet" et the section called "Conservation légale du verrouillage d'objet".

Les exemples suivants montrent comment créer un rôle AWS Identity and Access Management (IAM) avec des autorisations S3 Batch Operations et comment mettre à jour les autorisations du rôle pour inclure les `s3:PutObjectRetention` autorisations afin que vous puissiez exécuter la rétention S3 Object Lock sur les objets de votre compartiment manifeste. Vous devez également disposer d'un manifeste CSV qui identifie les objets de votre tâche d'opérations par lot S3. Pour de plus amples informations, veuillez consulter the section called "Spécification d'un manifeste".

Pour utiliser les exemples suivants, remplacez *`user input placeholders`* par vos propres informations.

À l'aide du AWS CLI

L' AWS CLI exemple suivant montre comment utiliser Batch Operations pour appliquer la rétention S3 Object Lock à plusieurs objets.

```
export AWS_PROFILE='aws-user'

read -d '' retention_permissions <<EOF
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": [
                "arn:aws:s3:::{{amzn-s3-demo-manifest-bucket}}/*"
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-
name retention-permissions --policy-document "${retention_permissions}"
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant montre comment utiliser Batch Operations pour appliquer la rétention S3 Object Lock à plusieurs objets.

```
public void allowPutObjectRetention() {
    final String roleName = "batch_operations-object-lock";

    final String retentionPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectRetention\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();
```

```
    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(retentionPermissions)
            .withPolicyName("retention-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

Utilisation de la fonctionnalité d'opérations par lot S3 avec le mode de conformité de rétention du verrouillage des objets S3

L'exemple suivant s'appuie sur les exemples précédents de création d'une stratégie d'approbation et de définition des autorisations de configuration pour les opérations par lot S3 et le verrouillage des objets S3 sur vos objets. Cet exemple définit le mode de conservation sur `COMPLIANCE` et fixe la date `retain until date` au 1er janvier 2025. Cet exemple crée une tâche qui cible les objets du compartiment manifeste et signale les résultats dans le compartiment de rapports que vous avez identifié.

Pour utiliser les exemples suivants, remplacez *`user input placeholders`* par vos propres informations.

À l'aide du AWS CLI

Les AWS CLI exemples suivants montrent comment utiliser Batch Operations pour appliquer le mode de conformité de rétention S3 Object Lock à plusieurs objets.

Example : défini le mode de conformité de rétention du verrouillage d'objet S3 sur plusieurs objets

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-01T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
```

```
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::ReportBucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "amzn-s3-demo-completion-report-bucket/compliance-objects-batch-
operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Set compliance retain-until to 1 Jul 2030";
```

Example — Prolonger la date **`retain until date`** du mode **`COMPLIANCE`** jusqu'au 15 janvier 2025

L'exemple suivant étend la `COMPLIANCE` du mode `retain until date` jusqu'au 15 janvier 2025.

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-15T00:00:00",
      "Mode":"COMPLIANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/compliance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/compliance-objects-batch_operations",
```

```
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Extend compliance retention to 15 Jan 2025";
```

Utilisation du AWS SDK pour Java

Les AWS SDK pour Java exemples suivants montrent comment utiliser Batch Operations pour appliquer le mode de conformité de rétention S3 Object Lock à plusieurs objets.

Example — Définir le mode de conservation sur CONFORMITÉ et fixer la date de fin de conservation au 1er janvier 2025

```
public String createComplianceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "your-object-version-Id";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);
```

```
    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-bops";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date janFirst = format.parse("01/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
                            .withRetainUntilDate(janFirst)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Set compliance retain-until to 1 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Example — Extension de la date **`retain until date`** du mode **`COMPLIANCE`**

L'exemple suivant étend la `retain until date` du mode `COMPLIANCE` jusqu'au 15 janvier 2025.

```
public String createExtendComplianceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
compliance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/compliance-objects-batch_operations";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan15th = format.parse("15/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.COMPLIANCE)
                            .withRetainUntilDate(jan15th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;
```

```
    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Extend compliance retention to 15 Jan 2025")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Utiliser la fonctionnalité d'opérations par lot S3 avec le mode de gouvernance de rétention du verrouillage des objets S3

L'exemple suivant s'appuie sur les exemples précédents de création d'une stratégie d'approbation et de définition des autorisations de configuration pour les opérations par lot S3 et le verrouillage des objets S3. Cet exemple illustre comment appliquer la gouvernance de conservation du verrouillage d'objet S3 avec la date `retain until date` fixée au 30 janvier 2025 sur plusieurs objets. Il crée une tâche d'opérations par lot qui utilise le compartiment manifeste et signale les résultats dans le compartiment de rapports.

Pour utiliser les exemples suivants, remplacez *`user input placeholders`* par vos propres informations.

À l'aide du AWS CLI

Les AWS CLI exemples suivants montrent comment utiliser Batch Operations pour appliquer le mode de gouvernance de rétention S3 Object Lock à plusieurs objets.

Example — Appliquer la gouvernance de conservation du verrouillage d'objet S3 sur plusieurs objets avec la date de fin de conservation fixée au 30 janvier 2025

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'
```

```
read -d '' OPERATION <<EOF
{
  "S3PutObjectRetention": {
    "Retention": {
      "RetainUntilDate":"2025-01-30T00:00:00",
      "Mode":"GOVERNANCE"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucketT",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/governance-objects",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
```

```
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Put governance retention";
```

Example — Contourner la gouvernance de conservation sur plusieurs objets

L'exemple suivant s'appuie sur les exemples précédents de création d'une stratégie d'approbation et de définition des autorisations de configuration pour les opérations par lot S3 et le verrouillage des objets S3. Il montre comment contourner la gouvernance de rétention entre plusieurs objets et crée une tâche d'opérations par lot qui utilise le compartiment manifeste et signale les résultats dans le compartiment de rapports.

```
export AWS_PROFILE='aws-user'

read -d '' bypass_governance_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:BypassGovernanceRetention"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        }
    ]
}
EOF

aws iam put-role-policy --role-name batch-operations-objectlock --policy-name bypass-
governance-permissions --policy-document "${bypass_governance_permissions}"

export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
```

```
  "S3PutObjectRetention": {
    "BypassGovernanceRetention": true,
    "Retention": {
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/governance-objects-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/batch_operations-governance",
  "ReportScope": "AllTasks"
}
EOF

aws \
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
```

```
    --region "${AWS_DEFAULT_REGION}" \
    --description "Remove governance retention";
```

Utilisation du AWS SDK pour Java

L'exemple suivant s'appuie sur les exemples précédents de création d'une stratégie d'approbation et de définition des autorisations de configuration pour les opérations par lot S3 et le verrouillage des objets S3. Cet exemple illustre comment appliquer la gouvernance de conservation du verrouillage d'objet S3 avec la date `retain until date` fixée au 30 janvier 2025 sur plusieurs objets. Cet exemple crée une tâche d'opérations par lot qui utilise le compartiment de manifeste et signale les résultats dans le compartiment de rapports.

Example — Appliquer la gouvernance de conservation du verrouillage d'objet S3 sur plusieurs objets avec la date de fin de conservation fixée au 30 janvier 2025

```
public String createGovernanceRetentionJob(final AWSS3ControlClient awss3ControlClient)
 throws ParseException {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/governance-objects";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
```

```
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final SimpleDateFormat format = new SimpleDateFormat("dd/MM/yyyy");
    final Date jan30th = format.parse("30/01/2025");

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()
                            .withMode(S3ObjectLockRetentionMode.GOVERNANCE)
                            .withRetainUntilDate(jan30th)));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Put governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Example — Contourner la gouvernance de conservation sur plusieurs objets

L'exemple suivant s'appuie sur les exemples précédents de création d'une stratégie d'approbation et de définition des autorisations de configuration pour les opérations par lot S3 et le verrouillage des objets S3. Cet exemple montre comment contourner la gouvernance de conservation entre plusieurs objets et crée une tâche d'opérations par lot qui utilise le compartiment de manifeste et signale les résultats dans le compartiment de rapports.

```
public void allowBypassGovernance() {
    final String roleName = "batch_operations-object-lock";
```

```
    final String bypassGovernancePermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:BypassGovernanceRetention\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(bypassGovernancePermissions)
            .withPolicyName("bypass-governance-permissions")
            .withRoleName(roleName);

    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
public String createRemoveGovernanceRetentionJob(final AWSS3ControlClient
 awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
governance-objects-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);
```

```
    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/batch_operations-governance";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectRetention(new S3SetObjectRetentionOperation()
                    .withRetention(new S3Retention()));

    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Remove governance retention")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Utilisation de la fonctionnalité d'opérations par lot S3 pour désactiver la conservation légale du verrouillage d'objet S3

L'exemple suivant s'appuie sur les exemples précédents de création d'une stratégie d'approbation et de définition des autorisations de configuration pour les opérations par lot S3 et le verrouillage des

objets S3. Cet exemple montre comment désactiver la conservation légale du verrouillage des objets à l'aide de la fonctionnalité d'opérations par lot.

Cet exemple met d'abord à jour le rôle afin d'accorder des autorisations `s3:PutObjectLegalHold`, crée une tâche d'opérations par lot qui désactive (supprime) la conservation légale des objets identifiés dans le manifeste, puis établit un rapport à ce sujet.

Pour utiliser les exemples suivants, remplacez *`user input placeholders`* par vos propres informations.

À l'aide du AWS CLI

Les AWS CLI exemples suivants montrent comment utiliser Batch Operations pour désactiver les blocages légaux de S3 Object Lock sur plusieurs objets.

Example — Met à jour le rôle pour accorder des autorisations **`s3:PutObjectLegalHold`**

```
export AWS_PROFILE='aws-user'

read -d '' legal_hold_permissions <<EOF
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObjectLegalHold"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
            ]
        }
    ]

EOF

aws iam put-role-policy --role-name batch_operations-objectlock --policy-name legal-
hold-permissions --policy-document "${legal_hold_permissions}"
```

Example — Désactiver la conservation légale

L'exemple suivant désactive la conservation légale.

```
export AWS_PROFILE='aws-user'
export AWS_DEFAULT_REGION='us-west-2'
export ACCOUNT_ID=123456789012
export ROLE_ARN='arn:aws:iam::123456789012:role/batch_operations-objectlock'

read -d '' OPERATION <<EOF
{
  "S3PutObjectLegalHold": {
    "LegalHold": {
      "Status":"OFF"
    }
  }
}
EOF

read -d '' MANIFEST <<EOF
{
  "Spec": {
    "Format": "S3BatchOperations_CSV_20180820",
    "Fields": [
      "Bucket",
      "Key"
    ]
  },
  "Location": {
    "ObjectArn": "arn:aws:s3:::amzn-s3-demo-manifest-bucket/legalhold-object-
manifest.csv",
    "ETag": "Your-manifest-ETag"
  }
}
EOF

read -d '' REPORT <<EOF
{
  "Bucket": "arn:aws:s3:::amzn-s3-demo-completion-report-bucket",
  "Format": "Report_CSV_20180820",
  "Enabled": true,
  "Prefix": "reports/legalhold-objects-batch_operations",
  "ReportScope": "AllTasks"
}
EOF

aws \
```

```
    s3control create-job \
    --account-id "${ACCOUNT_ID}" \
    --manifest "${MANIFEST//$'\n'}" \
    --operation "${OPERATION//$'\n'/}" \
    --report "${REPORT//$'\n'}" \
    --priority 10 \
    --role-arn "${ROLE_ARN}" \
    --client-request-token "$(uuidgen)" \
    --region "${AWS_DEFAULT_REGION}" \
    --description "Turn off legal hold";
```

Utilisation du AWS SDK pour Java

Les AWS SDK pour Java exemples suivants montrent comment utiliser Batch Operations pour désactiver les blocages légaux de S3 Object Lock sur plusieurs objets.

Example — Met à jour le rôle pour accorder des autorisations **`s3:PutObjectLegalHold`**

```
public void allowPutObjectLegalHold() {
    final String roleName = "batch_operations-object-lock";

    final String legalHoldPermissions = "{" +
            "    \"Version\": \"2012-10-17\"," +
            "    \"Statement\": [" +
            "        {" +
            "            \"Effect\": \"Allow\"," +
            "            \"Action\": [" +
            "                \"s3:PutObjectLegalHold\"" +
            "            ]," +
            "            \"Resource\": [" +
            "                \"arn:aws:s3:::amzn-s3-demo-manifest-bucket/*\"" +
            "            ]" +
            "        }" +
            "    ]" +
            "}";

    final AmazonIdentityManagement iam =
            AmazonIdentityManagementClientBuilder.defaultClient();

    final PutRolePolicyRequest putRolePolicyRequest = new PutRolePolicyRequest()
            .withPolicyDocument(legalHoldPermissions)
            .withPolicyName("legal-hold-permissions")
            .withRoleName(roleName);
```

```
    final PutRolePolicyResult putRolePolicyResult =
 iam.putRolePolicy(putRolePolicyRequest);
}
```

Example — Désactiver la conservation légale

Utilisez l'exemple ci-dessous si vous souhaitez désactiver la conservation légale.

```
public String createLegalHoldOffJob(final AWSS3ControlClient awss3ControlClient) {
    final String manifestObjectArn = "arn:aws:s3:::amzn-s3-demo-manifest-bucket/
legalhold-object-manifest.csv";
    final String manifestObjectVersionId = "15ad5ba069e6bbc465c77bf83d541385";

    final JobManifestLocation manifestLocation = new JobManifestLocation()
            .withObjectArn(manifestObjectArn)
            .withETag(manifestObjectVersionId);

    final JobManifestSpec manifestSpec =
            new JobManifestSpec()
                    .withFormat(JobManifestFormat.S3BatchOperations_CSV_20180820)
                    .withFields("Bucket", "Key");

    final JobManifest manifestToPublicApi = new JobManifest()
            .withLocation(manifestLocation)
            .withSpec(manifestSpec);

    final String jobReportBucketArn = "arn:aws:s3:::amzn-s3-demo-completion-report-
bucket";
    final String jobReportPrefix = "reports/legalhold-objects-batch_operations";

    final JobReport jobReport = new JobReport()
            .withEnabled(true)
            .withReportScope(JobReportScope.AllTasks)
            .withBucket(jobReportBucketArn)
            .withPrefix(jobReportPrefix)
            .withFormat(JobReportFormat.Report_CSV_20180820);

    final JobOperation jobOperation = new JobOperation()
            .withS3PutObjectLegalHold(new S3SetObjectLegalHoldOperation()
                    .withLegalHold(new S3ObjectLockLegalHold()
                            .withStatus(S3ObjectLockLegalHoldStatus.OFF)));
```

```
    final String roleArn = "arn:aws:iam::123456789012:role/batch_operations-object-
lock";
    final Boolean requiresConfirmation = true;
    final int priority = 10;

    final CreateJobRequest request = new CreateJobRequest()
            .withAccountId("123456789012")
            .withDescription("Turn off legal hold")
            .withManifest(manifestToPublicApi)
            .withOperation(jobOperation)
            .withPriority(priority)
            .withRoleArn(roleArn)
            .withReport(jobReport)
            .withConfirmationRequired(requiresConfirmation);

    final CreateJobResult result = awss3ControlClient.createJob(request);

    return result.getJobId();
}
```

Didacticiel : transcodage par lot de vidéos avec les opérations par lot S3

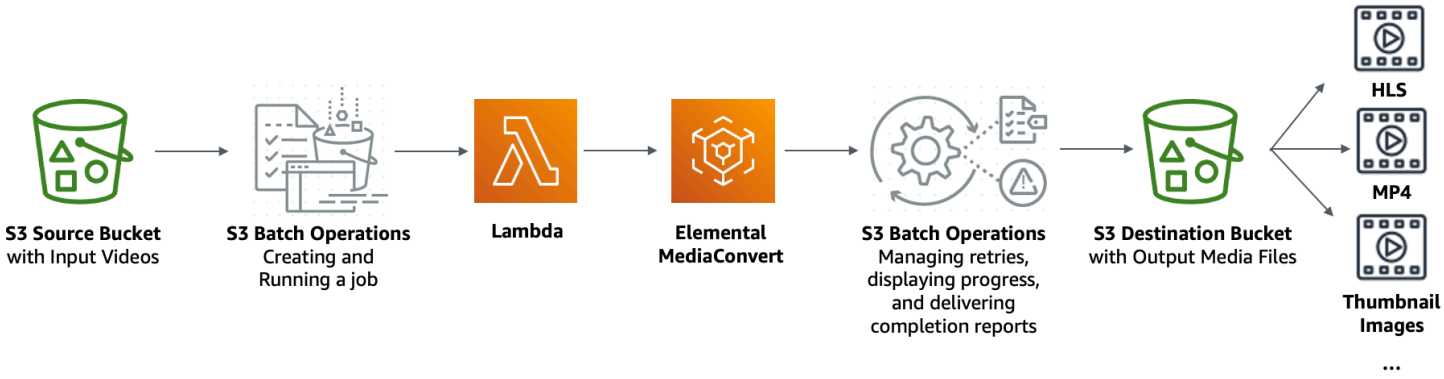
Les consommateurs de vidéos utilisent des appareils de toutes formes, tailles et millésimes pour profiter des contenus multimédia. Ce large éventail de services représente un défi pour les créateurs et distributeurs de contenus. Au lieu d'être dans un one-size-fits-all format, les vidéos doivent être converties afin qu'elles puissent couvrir une large gamme de tailles, de formats et de débits. Cette tâche de conversion est encore plus difficile lorsque vous avez un grand nombre de vidéos à convertir.

AWS vous propose une méthode pour créer une architecture distribuée évolutive qui effectue les opérations suivantes :

- Intégrer les vidéos d'entrée
- Traiter les vidéos en vue de leur lecture sur un large éventail d'appareils
- Stocker les fichiers multimédias transcodés
- Fournir les fichiers multimédias de sortie pour répondre à la demande

Si vous disposez de référentiels vidéo étendus stockés dans Amazon S3, vous pouvez transcoder ces vidéos à partir de leurs formats source en plusieurs types de fichiers dans la taille, la résolution et le format requis par un lecteur vidéo ou un appareil particulier. Plus précisément, S3 Batch

Operations vous fournit une solution pour invoquer AWS Lambda des fonctions pour les vidéos d'entrée existantes dans un compartiment source S3. Ensuite, les fonctions Lambda appellent AWS Elemental MediaConvert pour effectuer des tâches de transcodage de vidéos à grande échelle. Les fichiers multimédias de sortie convertis sont stockés dans un compartiment de destination S3.



Objectif

Dans ce didacticiel, vous apprendrez à configurer la fonctionnalité Opérations par lot S3 pour invoquer une fonction Lambda pour le transcodage par lots de vidéos stockées dans un compartiment source S3. La fonction Lambda appelle MediaConvert pour transcoder les vidéos. Les sorties de chaque vidéo dans le compartiment source S3 se présentent comme suit :

- Un flux à débit adaptatif HTTP Live Streaming (HLS) pour lecture sur des appareils de diverses tailles et des largeurs de bande passante variables
- Un fichier MP4 vidéo
- Images miniatures collectées à intervalles

Rubriques

- Prérequis
- Étape 1 : créer un compartiment S3 pour les fichiers multimédias de sortie
- Étape 2 : créer un rôle IAM pour MediaConvert
- Étape 3 : créer un rôle IAM pour votre fonction Lambda
- Étape 4 : créer une fonction Lambda pour le transcodage vidéo
- Étape 5 : configurer un inventaire Amazon S3 pour votre compartiment source S3
- Étape 6 : créer un rôle IAM pour S3 Batch Operations
- Étape 7 : configurer et exécuter une tâche S3 Batch Operations
- Étape 8 : vérifier les fichiers multimédias de sortie à partir de votre compartiment de destination S3

- Étape 9 : nettoyer
- Étapes suivantes

Prérequis

Avant de commencer à suivre ce didacticiel, vous devez disposer d'un compartiment source Amazon S3 (par exemple *amzn-s3-demo-source-bucket*) avec des vidéos à transcoder déjà stockées.

Vous pouvez donner un autre nom au compartiment si vous le souhaitez. Pour en savoir plus sur les règles d'attribution de noms de compartiment dans Amazon S3, consultez Règles de dénomination des compartiments à usage général.

Pour le compartiment source S3, conservez les paramètres associés aux Paramètres de blocage de l'accès public à ce compartiment définis pour les valeurs par défaut (Block all public access (Bloquer tous les accès publics) est activé). Pour plus d'informations, consultez Création d'un bucket à usage général.

Pour en savoir plus sur le téléchargement de vidéos vers le compartiment source S3, consultez Chargement d'objets. Lorsque vous téléchargez de nombreux fichiers vidéo volumineux sur S3, vous pouvez également utiliser Amazon S3 Transfer Acceleration pour configurer des transferts de fichiers rapides et sécurisés. Transfer Acceleration peut accélérer le chargement de vidéos vers votre compartiment S3 pour le transfert à longue distance de vidéos plus volumineuses. Pour plus d'informations, consultez Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.

Étape 1 : créer un compartiment S3 pour les fichiers multimédias de sortie

Dans cette étape, vous créez un compartiment de destination S3 pour stocker les fichiers multimédias de sortie convertis. Vous créez également une configuration CORS (Cross Origin Resource Sharing) pour autoriser l'accès croisé aux fichiers multimédias transcodés stockés dans votre compartiment de destination S3.

Sous-étapes

- Créer un compartiment pour les fichiers multimédias de sortie
- Ajouter une configuration CORS à un compartiment de sortie S3

Créer un compartiment pour les fichiers multimédias de sortie

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Choisissez Créer un compartiment.
4. Pour Bucket Name (Nom du compartiment), indiquez le nom de votre compartiment, (par exemple, *amzn-s3-demo-destination-bucket1*).
5. Pour Région, choisissez l' Région AWS endroit où vous souhaitez que le compartiment réside.
6. Pour garantir l'accès public à vos fichiers multimédias de sortie, dans Paramètres de blocage de l'accès public à ce compartiment, désactivez Bloquer tous les accès publics.

   > **Warning**
   >
   > Avant de terminer cette étape, revoyez Blocage de l'accès public à votre stockage Amazon S3 pour vous assurer que vous comprenez et acceptez les risques liés à l'autorisation d'accès public. Lorsque vous désactivez les paramètres de blocage de l'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tous les accès publics à vos compartiments.
   > Si vous ne souhaitez pas effacer les paramètres de blocage de l'accès public, vous pouvez utiliser Amazon CloudFront pour transmettre les fichiers multimédia transcodés aux spectateurs (utilisateurs finaux). Pour de plus amples informations, veuillez consulter Tutoriel : Hébergement de vidéos en streaming à la demande avec Amazon S3 CloudFront, Amazon et Amazon Route 53.

7. Cochez la case pour Je reconnais que les paramètres actuels pourraient rendre ce compartiment et les objets qu'il contient accessibles publiquement.
8. Conservez les paramètres restants définis sur les valeurs par défaut.
9. Choisissez Créer un compartiment.

Ajouter une configuration CORS à un compartiment de sortie S3

Une configuration JSON CORS définit un moyen pour les applications Web clientes (lecteurs vidéo dans ce contexte) chargées dans un domaine particulier de lire des fichiers multimédias de sortie transcodés dans un autre domaine.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment que vous avez créé précédemment (par ex., *amzn-s3-demo-destination-bucket1*).
4. Sélectionnez l'onglet Autorisations.
5. Dans la section Partage des ressources cross-origin (CORS), choisissez Modifier.
6. Dans la zone de texte de configuration CORS, copiez-collez la configuration CORS ci-dessous.

   La configuration CORS doit être au format JSON. Dans cet exemple, l'attribut `AllowedOrigins` utilise le caractère générique (*) pour spécifier toutes les origines. Si vous connaissez votre origine précise, vous pouvez restreindre l'attribut `AllowedOrigins` à l'URL de votre lecteur spécifique. Pour plus d'informations sur la configuration de cet attribut et d'autres, consultez Éléments d'une configuration CORS.

   ```
   [
       {
           "AllowedOrigins": [
               "*"
           ],
           "AllowedMethods": [
               "GET"
           ],
           "AllowedHeaders": [
               "*"
           ],
           "ExposeHeaders": []

       }
   ]
   ```

7. Sélectionnez Enregistrer les modifications.

Étape 2 : créer un rôle IAM pour MediaConvert

AWS Elemental MediaConvert Pour pouvoir transcoder des vidéos d'entrée stockées dans votre compartiment S3, vous devez disposer d'un rôle de service AWS Identity and Access Management (IAM) qui octroie MediaConvert les autorisations de lecture et d'écriture de fichiers vidéo depuis et

vers vos compartiments source et destination S3. Lorsque vous exécutez des tâches de transcodage, la MediaConvert console utilise ce rôle.

Pour créer un rôle IAM pour MediaConvert

1. Créez un rôle IAM avec un nom de rôle que vous choisissez (par exemple, **`tutorial-mediaconvert-role`**). Pour créer ce rôle, suivez les étapes décrites dans la section Créer votre MediaConvert rôle dans IAM (console) dans le guide de l'AWS Elemental MediaConvert utilisateur.
2. Après avoir créé le rôle IAM pour MediaConvert, dans la liste des rôles, choisissez le nom du rôle pour MediaConvert lequel vous avez créé (par exemple,**`tutorial-mediaconvert-role`**).
3. Dans la page Summary (Récapitulatif), copiez l'ARN du rôle (commençant par `arn:aws:iam::`), puis enregistrez l'ARN en vue d'une utilisation ultérieure.

   Pour plus d'informations ARNs, consultez Amazon Resource Names (ARNs) dans le manuel de référence AWS général.

Étape 3 : créer un rôle IAM pour votre fonction Lambda

Pour transcoder des vidéos par lots avec MediaConvert S3 Batch Operations, vous utilisez une fonction Lambda pour connecter ces deux services afin de convertir des vidéos. Cette fonction Lambda doit avoir un rôle IAM qui accorde à la fonction Lambda des autorisations d'accès et MediaConvert des opérations de traitement par lots S3.

Sous-étapes

- Créer un rôle IAM pour votre fonction Lambda
- Intégrez une politique en ligne pour le rôle IAM de votre fonction Lambda

Créer un rôle IAM pour votre fonction Lambda

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de gauche, choisissez Rôles, puis Créer un rôle.
3. Cliquez sur le type de rôle de service AWS , puis, sous Common use cases (Cas d'utilisation courants), choisissez Lambda.
4. Choisissez Suivant : Autorisations.

5. Sur la page Attach Permissions policies (Attacher les stratégies d'autorisations), saisissez **`AWSLambdaBasicExecutionRole`** dans la case Filter policies (Politiques de filtrage). Pour associer la politique gérée AWSLambdaBasicExecutionRoleà ce rôle afin d'accorder des autorisations d'écriture à Amazon CloudWatch Logs, cochez la case à côté de AWSLambdaBasicExecutionRole.
6. Choisissez Suivant.
7. Pour le Nom du rôle, saisissez **`tutorial-lambda-transcode-role`**.
8. (Facultatif) Ajoutez des balises à la stratégie gérée.
9. Choisissez Créer un rôle.

Intégrez une politique en ligne pour le rôle IAM de votre fonction Lambda

Pour accorder des autorisations à la MediaConvert ressource nécessaire à l'exécution de la fonction Lambda, vous devez utiliser une politique intégrée.

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de gauche, choisissez Rôles.
3. Dans la liste Roles (Rôles), choisissez le nom du rôle IAM que vous avez créé précédemment pour votre fonction Lambda (par exemple, **`tutorial-lambda-transcode-role`**).
4. Sélectionnez l'onglet Autorisations.
5. Sélectionnez Ajouter une politique en ligne.
6. Choisissez l'onglet JSON, puis copiez et collez la stratégie JSON suivante.

   Dans la politique JSON, remplacez l'exemple de valeur `Resource` d'ARN de par le rôle ARN du rôle IAM MediaConvert que vous avez créé à l'étape 2 (par exemple,**`tutorial-mediaconvert-role`**).

   JSON

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

```
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "Logging"
        },
        {
            "Action": [
                "iam:PassRole"
            ],
            "Resource": [
                "arn:aws:iam::111122223333:role/tutorial-mediaconvert-role"
            ],
            "Effect": "Allow",
            "Sid": "PassRole"
        },
        {
            "Action": [
                "mediaconvert:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "MediaConvertService"
        },
        {
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "*"
            ],
            "Effect": "Allow",
            "Sid": "S3Service"
        }
    ]
}
```

7. Choisissez Review Policy (Examiner une stratégie).
8. Pour Nom, saisissez **`tutorial-lambda-policy`**.
9. Choisissez Create Policy (Créer une politique).

Lorsque vous aurez créé une politique en ligne, elle sera automatiquement intégrée au rôle IAM de votre fonction Lambda.

Étape 4 : créer une fonction Lambda pour le transcodage vidéo

Dans cette section du didacticiel, vous allez créer une fonction Lambda à l'aide du SDK pour Python afin de l'intégrer à S3 Batch Operations et. MediaConvert Pour commencer à transcoder les vidéos déjà stockées dans votre compartiment source S3, vous exécutez une tâche d'opérations par lot S3 qui invoque directement la fonction Lambda pour chaque vidéo du compartiment source S3. Ensuite, la fonction Lambda soumet une tâche de transcodage pour chaque vidéo à. MediaConvert

Sous-étapes

- Écrire le code de la fonction Lambda et créer un package de déploiement
- Créer une fonction Lambda à l'aide d'un rôle d'exécution (console)
- Déployez votre fonction Lambda avec les archives de fichiers .zip, puis configurez la fonction Lambda (console)

Écrire le code de la fonction Lambda et créer un package de déploiement

1. Sur votre ordinateur local, créez un dossier nommé `batch-transcode`.
2. Dans le dossier `batch-transcode`, créez un fichier contenant les paramètres de la tâche JSON. Par exemple, vous pouvez utiliser les paramètres fournis dans cette section et nommer le fichier `job.json`.

   Un fichier `job.json` spécifie les éléments suivants :

   - Quels fichiers transcoder
   - Comment transcoder vos vidéos d'entrée
   - Quels fichiers multimédias de sortie vous souhaitez créer
   - Quel nom à attribuer aux fichiers transcodés
   - Où enregistrer les fichiers transcodés
   - Quelles fonctions avancées appliquer, et ainsi de suite

   Dans ce didacticiel, nous utiliserons le fichier `job.json` suivant pour créer les sorties suivantes pour chaque vidéo dans le compartiment source S3 :

- Un flux à débit adaptatif HTTP Live Streaming (HLS) pour lecture sur plusieurs appareils de diverses tailles et des largeurs de bande passante variables
- Un fichier MP4 vidéo
- Images miniatures collectées à intervalles

Ce fichier d'exemple `job.json` utilise le débit variable selon la qualité (QVBR) pour optimiser la qualité de la vidéo. La sortie HLS est conforme aux applications d'Apple (fichier audio séparé du fichier vidéo, durée de segment de 6 secondes et qualité vidéo optimisée via QVBR automatique).

Si vous ne souhaitez pas utiliser les exemples de paramètres fournis ici, vous pouvez générer une spécification `job.json` basée sur votre cas d'utilisation. Pour assurer la cohérence entre vos sorties, vérifiez que vos fichiers d'entrée ont des configurations vidéo et audio similaires. Créez des automatisations distinctes (paramètres `job.json` uniques) pour tous les fichiers d'entrée avec différentes configurations vidéo et audio. Pour plus d'informations, consultez Exemples de paramètres de tâche AWS Elemental MediaConvert en JSON dans le Guide de l'utilisateur AWS Elemental MediaConvert .

```
{
  "OutputGroups": [
    {
      "CustomName": "HLS",
      "Name": "Apple HLS",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
```

```
                483,
                484,
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
              ]
            }
          },
          "VideoDescription": {
            "Width": 640,
            "ScalingBehavior": "DEFAULT",
            "Height": 360,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "GopSize": 2,
                "Slices": 1,
                "GopBReference": "DISABLED",
                "MaxBitrate": 1200000,
                "SlowPal": "DISABLED",
                "SpatialAdaptiveQuantization": "ENABLED",
                "TemporalAdaptiveQuantization": "ENABLED",
                "FlickerAdaptiveQuantization": "DISABLED",
                "EntropyEncoding": "CABAC",
                "FramerateControl": "INITIALIZE_FROM_SOURCE",
                "RateControlMode": "QVBR",
                "CodecProfile": "MAIN",
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
```

```
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_360"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "TimedMetadataPid": 502,
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
```

```
                485,
                486,
                487,
                488,
                489,
                490,
                491,
                492
              ]
            }
          },
          "VideoDescription": {
            "Width": 960,
            "ScalingBehavior": "DEFAULT",
            "Height": 540,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "GopSize": 2,
                "Slices": 1,
                "GopBReference": "DISABLED",
                "MaxBitrate": 3500000,
                "SlowPal": "DISABLED",
                "SpatialAdaptiveQuantization": "ENABLED",
                "TemporalAdaptiveQuantization": "ENABLED",
                "FlickerAdaptiveQuantization": "DISABLED",
                "EntropyEncoding": "CABAC",
                "FramerateControl": "INITIALIZE_FROM_SOURCE",
                "RateControlMode": "QVBR",
                "CodecProfile": "MAIN",
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
```

```
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_540"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {
              "AudioFramesPerPes": 4,
              "PcrControl": "PCR_EVERY_PES_PACKET",
              "PmtPid": 480,
              "PrivateMetadataPid": 503,
              "ProgramNumber": 1,
              "PatInterval": 0,
              "PmtInterval": 0,
              "TimedMetadata": "NONE",
              "VideoPid": 481,
              "AudioPids": [
                482,
                483,
                484,
                485,
                486,
                487,
```

```
                488,
                489,
                490,
                491,
                492
              ]
            }
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "GopSize": 2,
                "Slices": 1,
                "GopBReference": "DISABLED",
                "MaxBitrate": 5000000,
                "SlowPal": "DISABLED",
                "SpatialAdaptiveQuantization": "ENABLED",
                "TemporalAdaptiveQuantization": "ENABLED",
                "FlickerAdaptiveQuantization": "DISABLED",
                "EntropyEncoding": "CABAC",
                "FramerateControl": "INITIALIZE_FROM_SOURCE",
                "RateControlMode": "QVBR",
                "CodecProfile": "MAIN",
                "Telecine": "NONE",
                "MinIInterval": 0,
                "AdaptiveQuantization": "HIGH",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "TRANSITION_DETECTION",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "FramerateConversionAlgorithm": "DUPLICATE_DROP",
                "UnregisteredSeiTimecode": "DISABLED",
```

```
                "GopSizeUnits": "SECONDS",
                "ParControl": "INITIALIZE_FROM_SOURCE",
                "NumberBFramesBetweenReferenceFrames": 2,
                "RepeatPps": "DISABLED"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioRenditionSets": "program_audio",
              "SegmentModifier": "$dt$",
              "IFrameOnlyManifest": "EXCLUDE"
            }
          },
          "NameModifier": "_720"
        },
        {
          "ContainerSettings": {
            "Container": "M3U8",
            "M3u8Settings": {}
          },
          "AudioDescriptions": [
            {
              "AudioSourceName": "Audio Selector 1",
              "CodecSettings": {
                "Codec": "AAC",
                "AacSettings": {
                  "Bitrate": 96000,
                  "CodingMode": "CODING_MODE_2_0",
                  "SampleRate": 48000
                }
              }
            }
          ],
          "OutputSettings": {
            "HlsSettings": {
              "AudioGroupId": "program_audio",
              "AudioTrackType": "ALTERNATE_AUDIO_AUTO_SELECT_DEFAULT"
            }
```

```
          },
          "NameModifier": "_audio"
        }
      ],
      "OutputGroupSettings": {
        "Type": "HLS_GROUP_SETTINGS",
        "HlsGroupSettings": {
          "ManifestDurationFormat": "INTEGER",
          "SegmentLength": 6,
          "TimedMetadataId3Period": 10,
          "CaptionLanguageSetting": "OMIT",
          "Destination": "s3://EXAMPLE-BUCKET/HLS/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          },
          "TimedMetadataId3Frame": "PRIV",
          "CodecSpecification": "RFC_4281",
          "OutputSelection": "MANIFESTS_AND_SEGMENTS",
          "ProgramDateTimePeriod": 600,
          "MinSegmentLength": 0,
          "DirectoryStructure": "SINGLE_DIRECTORY",
          "ProgramDateTime": "EXCLUDE",
          "SegmentControl": "SEGMENTED_FILES",
          "ManifestCompression": "NONE",
          "ClientCache": "ENABLED",
          "StreamInfResolution": "INCLUDE"
        }
      }
    },
    {
      "CustomName": "MP4",
      "Name": "File Group",
      "Outputs": [
        {
          "ContainerSettings": {
            "Container": "MP4",
            "Mp4Settings": {
              "CslgAtom": "INCLUDE",
              "FreeSpaceBox": "EXCLUDE",
              "MoovPlacement": "PROGRESSIVE_DOWNLOAD"
```

```
            }
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 100,
            "CodecSettings": {
              "Codec": "H_264",
              "H264Settings": {
                "InterlaceMode": "PROGRESSIVE",
                "ParNumerator": 1,
                "NumberReferenceFrames": 3,
                "Syntax": "DEFAULT",
                "Softness": 0,
                "GopClosedCadence": 1,
                "HrdBufferInitialFillPercentage": 90,
                "GopSize": 2,
                "Slices": 2,
                "GopBReference": "ENABLED",
                "HrdBufferSize": 10000000,
                "MaxBitrate": 5000000,
                "ParDenominator": 1,
                "EntropyEncoding": "CABAC",
                "RateControlMode": "QVBR",
                "CodecProfile": "HIGH",
                "MinIInterval": 0,
                "AdaptiveQuantization": "AUTO",
                "CodecLevel": "AUTO",
                "FieldEncoding": "PAFF",
                "SceneChangeDetect": "ENABLED",
                "QualityTuningLevel": "SINGLE_PASS_HQ",
                "UnregisteredSeiTimecode": "DISABLED",
                "GopSizeUnits": "SECONDS",
                "ParControl": "SPECIFIED",
                "NumberBFramesBetweenReferenceFrames": 3,
                "RepeatPps": "DISABLED",
                "DynamicSubGop": "ADAPTIVE"
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
```

```
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          },
          "AudioDescriptions": [
            {
              "AudioTypeControl": "FOLLOW_INPUT",
              "AudioSourceName": "Audio Selector 1",
              "CodecSettings": {
                "Codec": "AAC",
                "AacSettings": {
                  "AudioDescriptionBroadcasterMix": "NORMAL",
                  "Bitrate": 160000,
                  "RateControlMode": "CBR",
                  "CodecProfile": "LC",
                  "CodingMode": "CODING_MODE_2_0",
                  "RawFormat": "NONE",
                  "SampleRate": 48000,
                  "Specification": "MPEG4"
                }
              },
              "LanguageCodeControl": "FOLLOW_INPUT",
              "AudioType": 0
            }
          ]
        }
      ],
      "OutputGroupSettings": {
        "Type": "FILE_GROUP_SETTINGS",
        "FileGroupSettings": {
          "Destination": "s3://EXAMPLE-BUCKET/MP4/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          }
        }
      }
    },
    {
      "CustomName": "Thumbnails",
      "Name": "File Group",
      "Outputs": [
```

```
        {
          "ContainerSettings": {
            "Container": "RAW"
          },
          "VideoDescription": {
            "Width": 1280,
            "ScalingBehavior": "DEFAULT",
            "Height": 720,
            "TimecodeInsertion": "DISABLED",
            "AntiAlias": "ENABLED",
            "Sharpness": 50,
            "CodecSettings": {
              "Codec": "FRAME_CAPTURE",
              "FrameCaptureSettings": {
                "FramerateNumerator": 1,
                "FramerateDenominator": 5,
                "MaxCaptures": 500,
                "Quality": 80
              }
            },
            "AfdSignaling": "NONE",
            "DropFrameTimecode": "ENABLED",
            "RespondToAfd": "NONE",
            "ColorMetadata": "INSERT"
          }
        }
      ],
      "OutputGroupSettings": {
        "Type": "FILE_GROUP_SETTINGS",
        "FileGroupSettings": {
          "Destination": "s3://EXAMPLE-BUCKET/Thumbnails/",
          "DestinationSettings": {
            "S3Settings": {
              "AccessControl": {
                "CannedAcl": "PUBLIC_READ"
              }
            }
          }
        }
      }
    }
  ],
  "AdAvailOffset": 0,
  "Inputs": [
```

```
    {
      "AudioSelectors": {
        "Audio Selector 1": {
          "Offset": 0,
          "DefaultSelection": "DEFAULT",
          "ProgramSelection": 1
        }
      },
      "VideoSelector": {
        "ColorSpace": "FOLLOW"
      },
      "FilterEnable": "AUTO",
      "PsiControl": "USE_PSI",
      "FilterStrength": 0,
      "DeblockFilter": "DISABLED",
      "DenoiseFilter": "DISABLED",
      "TimecodeSource": "EMBEDDED",
      "FileInput": "s3://EXAMPLE-INPUT-BUCKET/input.mp4"
    }
  ]
}
```

3. Dans le dossier `batch-transcode`, créez un fichier avec une fonction Lambda. Vous pouvez utiliser l'exemple Python suivant et nommer le fichier `convert.py`.

   S3 Batch Operations envoie des données propres à la tâche à une fonction Lambda et demande des données de résultat en retour. Pour consulter des exemples de requête et de réponse pour la fonction Lambda, des informations sur les codes de réponse et de résultat, ainsi que des exemples de fonctions Lambda pour S3 Batch Operations, consultez AWS Lambda Fonction Invoke.

```
import json
import os
from urllib.parse import urlparse
import uuid
import boto3

"""
When you run an S3 Batch Operations job, your job
invokes this Lambda function. Specifically, the Lambda function is
invoked on each video object listed in the manifest that you specify
for the S3 Batch Operations job in Step 5.
```

```
Input parameter "event": The S3 Batch Operations event as a request
                         for the Lambda function.

Input parameter "context": Context about the event.

Output: A result structure that Amazon S3 uses to interpret the result
        of the operation. It is a job response returned back to S3 Batch
 Operations.
"""
def handler(event, context):

    invocation_schema_version = event['invocationSchemaVersion']
    invocation_id = event['invocationId']
    task_id = event['tasks'][0]['taskId']

    source_s3_key = event['tasks'][0]['s3Key']
    source_s3_bucket = event['tasks'][0]['s3BucketArn'].split(':::')[-1]
    source_s3 = 's3://' + source_s3_bucket + '/' + source_s3_key

    result_list = []
    result_code = 'Succeeded'
    result_string = 'The input video object was converted successfully.'

    # The type of output group determines which media players can play
    # the files transcoded by MediaConvert.
    # For more information, see Creating outputs with AWS Elemental MediaConvert.
    output_group_type_dict = {
        'HLS_GROUP_SETTINGS': 'HlsGroupSettings',
        'FILE_GROUP_SETTINGS': 'FileGroupSettings',
        'CMAF_GROUP_SETTINGS': 'CmafGroupSettings',
        'DASH_ISO_GROUP_SETTINGS': 'DashIsoGroupSettings',
        'MS_SMOOTH_GROUP_SETTINGS': 'MsSmoothGroupSettings'
    }

    try:
        job_name = 'Default'
        with open('job.json') as file:
            job_settings = json.load(file)

        job_settings['Inputs'][0]['FileInput'] = source_s3

        # The path of each output video is constructed based on the values of
        # the attributes in each object of OutputGroups in the job.json file.
        destination_s3 = 's3://{0}/{1}/{2}' \
```

```
            .format(os.environ['amzn-s3-demo-destination-bucket'],
                    os.path.splitext(os.path.basename(source_s3_key))[0],
                    os.path.splitext(os.path.basename(job_name))[0])

        for output_group in job_settings['OutputGroups']:
            output_group_type = output_group['OutputGroupSettings']['Type']
            if output_group_type in output_group_type_dict.keys():
                output_group_type = output_group_type_dict[output_group_type]
                output_group['OutputGroupSettings'][output_group_type]
['Destination'] = \
                    "{0}{1}".format(destination_s3,
                                    urlparse(output_group['OutputGroupSettings']
[output_group_type]['Destination']).path)
            else:
                raise ValueError("Exception: Unknown Output Group Type {}."
                                 .format(output_group_type))

        job_metadata_dict = {
            'assetID': str(uuid.uuid4()),
            'application': os.environ['Application'],
            'input': source_s3,
            'settings': job_name
        }

        region = os.environ['AWS_DEFAULT_REGION']
        endpoints = boto3.client('mediaconvert', region_name=region) \
            .describe_endpoints()
        client = boto3.client('mediaconvert', region_name=region,
                              endpoint_url=endpoints['Endpoints'][0]['Url'],
                              verify=False)

        try:
            client.create_job(Role=os.environ['MediaConvertRole'],
                              UserMetadata=job_metadata_dict,
                              Settings=job_settings)
        # You can customize error handling based on different error codes that
        # MediaConvert can return.
        # For more information, see MediaConvert error codes.
        # When the result_code is TemporaryFailure, S3 Batch Operations retries
        # the task before the job is completed. If this is the final retry,
        # the error message is included in the final report.
        except Exception as error:
            result_code = 'TemporaryFailure'
            raise
```

```
    except Exception as error:
        if result_code != 'TemporaryFailure':
            result_code = 'PermanentFailure'
        result_string = str(error)

    finally:
        result_list.append({
            'taskId': task_id,
            'resultCode': result_code,
            'resultString': result_string,
        })

    return {
        'invocationSchemaVersion': invocation_schema_version,
        'treatMissingKeyAs': 'PermanentFailure',
        'invocationId': invocation_id,
        'results': result_list
    }
```

4. Pour créer un package de déploiement avec `convert.py` et `job.json` sous forme de fichier `.zip` nommé `lambda.zip`, dans votre terminal local, ouvrez le dossier `batch-transcode` que vous avez créé précédemment et exécutez la commande suivante.

   Pour les utilisateurs macOS, exécutez la commande suivante :

   ```
   zip -r lambda.zip convert.py job.json
   ```

   Pour les utilisateurs Windows, exécutez les commandes suivantes :

   ```
   powershell Compress-Archive convert.py lambda.zip
   ```

   ```
   powershell Compress-Archive -update job.json lambda.zip
   ```

Créer une fonction Lambda à l'aide d'un rôle d'exécution (console)

1. Ouvrez la AWS Lambda console à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le volet de navigation de gauche, choisissez Fonctions.
3. Choisissez Créer une fonction.

4. Choisissez Créer à partir de zéro.
5. Sous Informations de base, procédez comme suit :
   a. Sous Nom de la fonction, saisissez **`tutorial-lambda-convert`**.
   b. Pour Runtime, choisissez Python 3.13.
6. Choisissez Modifier le rôle d'exécution par défaut et, sous Rôle d'exécution, choisissez Utiliser un rôle existant.
7. Sous Existing role (Rôle existant), choisissez le nom du rôle IAM que vous avez créé pour votre fonction Lambda à l'étape 3 (par exemple, **`tutorial-lambda-transcode-role`**).
8. Pour les paramètres restants, conservez les paramètres par défaut.
9. Choisissez Créer une fonction.

Déployez votre fonction Lambda avec les archives de fichiers .zip, puis configurez la fonction Lambda (console)

1. Dans la section Code Source (Source du code) de la page de la fonction Lambda que vous avez créée (par exemple, **`tutorial-lambda-convert`**), choisissez Upload from (Télécharger à partir de), puis le fichier .zip.
2. Choisissez Charger pour sélectionner votre fichier `.zip` local.
3. Choisissez le fichier `lambda.zip` que vous avez créé précédemment, puis choisissez Open (Ouvrir).
4. Choisissez Enregistrer.
5. Dans la section Paramètres d'exécution, choisissez Modifier.
6. Pour indiquer à l'exécution Lambda la méthode de gestionnaire dans votre code de fonction Lambda à invoquer, saisissez **`convert.handler`** dans le champ Gestionnaire.

   Quand vous configurez une fonction dans Python, la valeur du paramètre de gestionnaire correspond au nom de fichier et au nom de module de gestionnaire, séparés par un point (`.`). Par exemple, `convert.handler` appelle la méthode `handler` définie dans le fichier `convert.py`.
7. Choisissez Enregistrer.
8. Dans la page de la fonction Lambda, choisissez l'onglet Configuration. Dans le volet de navigation de gauche de l'onglet Configuration, choisissez Variables d'environnement, puis Modifier.

9. Choisissez Ajouter une variable d'environnement. Ensuite, saisissez la clé et la valeur spécifiées pour chacune des variables d'environnement suivantes :

   - Clé : Valeur **`DestinationBucket`** : **`amzn-s3-demo-destination-bucket1`**

     Cette valeur est le compartiment S3 pour les fichiers multimédias de sortie que vous avez créés à l'étape 1.
   - Clé : Valeur **`MediaConvertRole`** : **`arn:aws:iam::`*`111122223333`*`:role/tutorial-mediaconvert-role`**

     Cette valeur est l'ARN du rôle IAM MediaConvert que vous avez créé à l'étape 2. Assurez-vous de remplacer cet ARN par le véritable ARN de votre rôle IAM.
   - Clé : Valeur **`Application`** : **`Batch-Transcoding`**

     Cette valeur est le nom de l'application.
10. Choisissez Enregistrer.
11. (Facultatif) Dans l'onglet Configuration, dans la section Configuration générale du volet de navigation de gauche, choisissez Modifier. Dans le champ Délai d'expiration, saisissez **2** min **0** sec. Ensuite, choisissez Enregistrer.

    Le Délai d'expiration est le temps que Lambda autorise pour l'exécution d'une fonction avant de l'arrêter. Le durée par défaut est de 3 secondes. La tarification est basée sur la quantité de mémoire configurée et la durée pendant laquelle votre code s'exécute. Pour en savoir plus, consultez Pricing AWS Lambda (Tarification).

Étape 5 : configurer un inventaire Amazon S3 pour votre compartiment source S3

Après avoir configuré la fonction Lambda de transcodage, créez une tâche S3 Batch Operations pour transcoder un jeu de vidéos. Tout d'abord, vous avez besoin d'une liste d'objets vidéo d'entrée sur lesquels S3 Batch Operations devra exécuter l'action de transcodage indiquée. Pour obtenir une liste d'objets vidéo d'entrée, vous pouvez générer un rapport d'inventaire S3 pour votre compartiment source S3 (par exemple, *`amzn-s3-demo-source-bucket`*).

Sous-étapes

- Créer et configurer un compartiment pour les rapports d'inventaire S3 des vidéos d'entrée
- Configurer l'inventaire Amazon S3 pour votre compartiment source S3 des vidéos
- Consultez le rapport d'inventaire pour votre compartiment source S3 de vidéos

Créer et configurer un compartiment pour les rapports d'inventaire S3 des vidéos d'entrée

Pour stocker un rapport d'inventaire S3 qui répertorie les objets du compartiment source S3, créez un compartiment de destination d'inventaire S3, puis configurez une politique de compartiment pour que le compartiment puisse écrire des fichiers d'inventaire dans le compartiment source S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Choisissez Créer un compartiment.
4. Pour Bucket Name (Nom du compartiment), indiquez le nom de votre compartiment, (par exemple, *amzn-s3-demo-destination-bucket2*).
5. Pour Région AWS, choisissez l' Région AWS endroit où vous souhaitez que le compartiment réside.

   Le compartiment de destination de l'inventaire doit se trouver dans le même compartiment Région AWS que le compartiment source dans lequel vous configurez S3 Inventory. Le compartiment de destination d'inventaire peut être dans un autre Compte AWS.
6. Dans Block Public Access settings for this bucket (Bloquer les paramètres d'accès public pour ce compartiment), conservez les paramètres par défaut (Block all public access Bloquer tous les accès publics) est activé).
7. Pour les paramètres restants, conservez les paramètres par défaut.
8. Choisissez Créer un compartiment.
9. Dans la liste Compartiments, choisissez le nom du compartiment que vous venez de créer (par exemple, *amzn-s3-demo-destination-bucket2*).
10. Pour accorder à Amazon S3 l'autorisation d'écrire des données pour les rapports d'inventaire dans le compartiment de destination d'inventaire S3, choisissez l'onglet Permissions (Autorisations).
11. Faites défiler jusqu'à la section Stratégie de compartiment, puis choisissez Modifier. La page Stratégie de compartiment s'ouvre.
12. Pour accorder des autorisations pour l'inventaire S3, dans le champ Policy (Stratégie), collez la politique de compartiment suivante.

    Remplacez les trois exemples de valeurs par les valeurs suivantes :

- Le nom du compartiment que vous avez créé pour stocker les rapports d'inventaire (par exemple, *amzn-s3-demo-destination-bucket2*).
- Le nom du compartiment source qui stocke les vidéos d'entrée (par exemple, *amzn-s3-demo-source-bucket*).
- L' Compte AWS ID que vous avez utilisé pour créer le compartiment de source vidéo S3 (par exemple,*111122223333*.

JSON

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"InventoryAndAnalyticsExamplePolicy",
      "Effect":"Allow",
      "Principal": {"Service": "s3.amazonaws.com"},
      "Action":"s3:PutObject",
      "Resource":["arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"],
      "Condition": {
          "ArnLike": {
              "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
           },
         "StringEquals": {
             "aws:SourceAccount": "111122223333",
             "s3:x-amz-acl": "bucket-owner-full-control"
          }
       }
    }
  ]
}
```

13. Sélectionnez Enregistrer les modifications.

Configurer l'inventaire Amazon S3 pour votre compartiment source S3 des vidéos

Pour générer une liste de fichiers plats d'objets vidéo et de métadonnées, vous devez configurer l'inventaire S3 pour votre compartiment source S3 des vidéos. Ces rapports d'inventaire planifiés

peuvent inclure tous les objets du compartiment ou les objets regroupés par un préfixe partagé. Dans ce didacticiel, le rapport d'inventaire S3 inclut tous les objets vidéo de votre compartiment source S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Pour configurer un rapport d'inventaire S3 des vidéos d'entrée dans votre compartiment source S3, dans la liste Compartiments, choisissez le nom du compartiment source S3 (par exemple, *amzn-s3-demo-source-bucket*).
4. Choisissez l'onglet Gestion.
5. Faites défiler jusqu'à la section Inventory configurations (Configurations d'inventaire) et choisissez Create inventory configuration (Créer une configuration d'inventaire).
6. Pour le Nom de la configuration d'inventaire, saisissez un nom (par exemple, **`tutorial-inventory-config`**).
7. Sous Inventory scope (Portée de l'inventaire), choisissez Current version only (Version actuelle uniquement pour Object versions (Versions d'un objet) et conservez les autres paramètres Inventory scope (Portée de l'inventaire) définis pour les valeurs par défaut de ce didacticiel.
8. Dans la section Report details (Détails du rapport), pour Destination bucket (Compartiment de destination), choisissez This account (Ce compte).
9. Pour Destination, choisissez Browse S3 (Parcourir S3), puis choisissez le compartiment de destination que vous avez créé précédemment pour enregistrer les rapports d'inventaire (par exemple, *amzn-s3-demo-destination-bucket2*). Ensuite, choisissez Choose path (Choisir un chemin).

   Le compartiment de destination de l'inventaire doit se trouver dans le même compartiment Région AWS que le compartiment source dans lequel vous configurez S3 Inventory. Le compartiment de destination d'inventaire peut être dans un autre Compte AWS.

   Sous le champ du compartiment Destination, l'autorisation du compartiment de destination est ajoutée à la politique du compartiment de destination afin de permettre à Amazon S3 de placer des données dans le compartiment de destination d'inventaire. Pour plus d'informations, consultez Création d'une politique de compartiment de destination.
10. Pour Frequency (Fréquence), choisissez Daily (Quotidiennement).
11. Pour Output format (Format de sortie), choisissez CSV.
12. Pour Statut, choisissez Activer.

13. Dans la section Server-side encryption (Chiffrement côté serveur), choisissez Disable (Désactiver) pour ce didacticiel.

    Pour plus d'informations, consultez Configuration de l'inventaire à l'aide de la console S3 et Octroi à Amazon S3 d'utiliser votre clé gérée par le client pour le chiffrement.

14. Dans la section Additional fields - optional (Champs supplémentaires – facultatif), sélectionnez Size (Taille) Last modified (Dernière modification) et Storage class (Classe de stockage).
15. Choisissez Créer.

Pour plus d'informations, consultez Configuration de l'inventaire à l'aide de la console S3.

Consultez le rapport d'inventaire pour votre compartiment source S3 de vidéos

Lorsqu'un rapport d'inventaire est publié, les fichiers manifestes sont envoyés au compartiment de destination d'inventaire S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste des Compartiments, choisissez le nom du compartiment source des vidéos (par exemple, *amzn-s3-demo-source-bucket*).
4. Choisissez Gestion.
5. Pour savoir si votre rapport d'inventaire S3 est prêt afin que vous puissiez créer une tâche S3 Batch Operations à l'étape 7, sous Inventory configurations (Configurations d'inventaire), vérifiez si le bouton Create job from manifest (Créer une tâche à partir du manifeste) est activé.

   > **Note**
   >
   > La distribution du premier rapport d'inventaire peut prendre jusqu'à 48 heures. Si l'icône Créer une tâche à partir du manifeste est désactivé, cela signifie que le premier rapport d'inventaire n'a pas été remis. Attendez que le premier rapport d'inventaire soit livré et que le bouton Create job from manifest (Créer une tâche à partir du manifeste) soit activé pour créer une tâche S3 Batch Operations à l'étape 7.

6. Pour vérifier un rapport d'inventaire S3 (`manifest.json`), dans la colonne Destination, choisissez le nom du compartiment de destination d'inventaire que vous avez créé

précédemment pour stocker les rapports d'inventaire (par exemple, *amzn-s3-demo-destination-bucket2*).

7. Dans l'onglet Objects (Objets), choisissez le dossier existant portant le nom de votre compartiment source S3 (par exemple, *amzn-s3-demo-source-bucket*). Choisissez ensuite le nom dans lequel vous avez saisi dans Inventory configuration name (Nom de configuration d'inventaire) lorsque vous avez créé la configuration d'inventaire précédemment (par exemple, **tutorial-inventory-config**).

   Vous pouvez afficher une liste de dossiers avec les dates de génération des rapports en guise de noms.
8. Pour vérifier le rapport d'inventaire quotidien S3 à une date donnée, choisissez le dossier avec le nom de date de génération correspondant, puis choisissez `manifest.json`.
9. Pour vérifier les détails du rapport d'inventaire à une date précise, dans la page manifest.json, choisissez Télécharger ou Ouvrir.

Étape 6 : créer un rôle IAM pour S3 Batch Operations

Pour utiliser S3 Batch Operations à des fins de transcodage par lots, vous devez d'abord créer un rôle IAM pour permettre à Amazon S3 d'exécuter S3 Batch Operations.

Sous-étapes

- Créer une politique IAM pour S3 Batch Operations
- Créez un rôle IAM S3 Batch Operations et attachez les politiques d'autorisations

Créer une politique IAM pour S3 Batch Operations

Vous devez créer une politique IAM qui autorise la fonctionnalité Opérations par lot S3 à lire le manifeste d'entrée, invoquer la fonction Lambda et écrire le rapport de fin de tâche d'opérations par lot S3.

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de gauche, choisissez Politiques.
3. Choisissez Créer une politique.
4. Choisissez l'onglet JSON.
5. Dans le champ JSON, collez la politique JSON suivante.

Dans la stratégie JSON, remplacez les quatre valeurs d'exemple par les valeurs suivantes :

- Le nom du compartiment source qui stocke vos vidéos d'entrée (par exemple, *amzn-s3-demo-source-bucket*).
- Le nom du compartiment de destination d'inventaire que vous avez créé à l'étape 5 pour stocker des fichiers `manifest.json` (par exemple, *amzn-s3-demo-destination-bucket2*).
- Le nom du compartiment que vous avez créé à l'étape 1 pour stocker des fichiers multimédias de sortie (par exemple, *amzn-s3-demo-destination-bucket1*). Dans ce didacticiel, nous mettons les rapports de fin de tâche dans le compartiment de destination des fichiers multimédias de sortie.
- L'ARN du rôle de la fonction Lambda que vous avez créée à l'étape 4. Pour rechercher et copier l'ARN de rôle de la fonction Lambda, procédez comme suit :
  - Dans un nouvel onglet du navigateur, ouvrez la page Functions (Fonctions) de la console Lambda à l'adresse https://console.aws.amazon.com/lambda/home#/functions.
  - Dans la liste Functions (Fonctions), choisissez le nom de la fonction Lambda que vous avez créée à l'étape 4 (par exemple, **`tutorial-lambda-convert`**).
  - Choisissez Copier l'ARN.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Get",
            "Effect": "Allow",
            "Action": [
                "s3:GetObject",
                "s3:GetObjectVersion"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
                "arn:aws:s3:::amzn-s3-demo-destination-bucket2/*"
            ]
        },
        {
```

```
            "Sid": "S3PutJobCompletionReport",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket1/*"
        },
        {
            "Sid": "S3BatchOperationsInvokeLambda",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:us-west-2:111122223333:function:tutorial-
lambda-convert"
            ]
        }
    ]
}
```

6. Choisissez Étape suivante : balises.
7. Choisissez Étape suivante : vérification).
8. Dans le champ Nom, saisissez **`tutorial-s3batch-policy`**.
9. Choisissez Create Policy (Créer une politique).

Créez un rôle IAM S3 Batch Operations et attachez les politiques d'autorisations

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation de gauche, choisissez Roles (Rôles), puis Create role (Créer un rôle).
3. Choisissez le type de rôle Service AWS, puis le service S3.
4. Sous Sélectionner votre cas d'utilisation, choisissez S3 Batch Operations.
5. Choisissez Suivant.
6. Sous Autorisations d'attachement, entrez le nom de la stratégie IAM que vous avez créée précédemment (par exemple,**`tutorial-s3batch-policy`**) dans le champ de recherche pour filtrer la liste des politiques. Cochez la case en regard du nom de la stratégie (par exemple, **`tutorial-s3batch-policy`**).
7. Choisissez Suivant.

8. Pour le Nom du rôle, saisissez **`tutorial-s3batch-role`**.
9. Choisissez Créer un rôle.

   Après avoir créé le rôle IAM pour S3 Batch Operations, la politique de confiance suivante sera automatiquement attachée au rôle. Cette stratégie d'approbation permet au principal du service S3 Batch Operations d'assumer le rôle IAM.

   JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Étape 7 : configurer et exécuter une tâche S3 Batch Operations

Pour créer une tâche S3 Batch Operations aux fins de traiter les vidéos d'entrée dans votre compartiment source S3, vous devez préciser des paramètres pour cette tâche particulière.

> **Note**
>
> Avant de commencer à créer une tâche S3 Batch Operations, vérifiez que le bouton Create job from manifest (Créer une tâche à partir du manifeste) est activé. Pour plus d'informations, consultez Consultez le rapport d'inventaire pour votre compartiment source S3 de vidéos. Si le bouton Create job from manifest (Créer une tâche à partir du manifeste) est désactivé, cela signifie que le premier rapport d'inventaire n'a pas été livré et vous devez attendre que le bouton soit activé. Après avoir configuré l'inventaire Amazon S3 pour votre compartiment source S3 à l'étape 5, la livraison du premier rapport d'inventaire peut prendre jusqu'à 48 heures.

Sous-étapes

- Créer une tâche S3 Batch Operations
- Exécutez la tâche d'opérations par lot S3 pour invoquer votre fonction Lambda
- (Facultatif) Vérifiez votre rapport d'achèvement
- (Facultatif) Contrôlez chaque invocation Lambda dans la console Lambda
- (Facultatif) Surveillez chaque tâche de MediaConvert transcodage vidéo dans la console MediaConvert

Créer une tâche S3 Batch Operations

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Opérations par lot.
3. Choisissez Créer une tâche.
4. Pour Région AWS, choisissez la Région dans laquelle vous souhaitez créer votre tâche.

   Dans ce didacticiel, pour utiliser la tâche d'opérations par lot S3 aux fins d'invoquer une fonction Lambda, vous devez créer la tâche dans la même Région que le compartiment de source S3 des vidéos où se trouvent les objets référencés dans le manifeste.
5. Dans la section Manifest (Manifeste), procédez comme suit :

   a. Pour Manifest format (Format du manifeste), choisissez S3 Inventory report (manifest.json) (Rapport d'inventaire S3 [manifest.json]).

   b. Pour Manifest object (Objet du manifeste), choisissez Browse S3 (Parcourir S3) pour chercher le compartiment que vous avez créé à l'étape 5 pour stocker des rapports d'inventaire (par exemple, *`amzn-s3-demo-destination-bucket2`*). Sur la page Manifest object (Objet manifeste), parcourez les noms des objets jusqu'à ce que vous trouviez un fichier `manifest.json` pour une date spécifique. Ce fichier répertorie les informations sur toutes les vidéos que vous souhaitez transcoder par lots. Lorsque vous avez trouvé le fichier `manifest.json` que vous souhaitez utiliser, choisissez le bouton d'option en regard de celui-ci. Ensuite, choisissez Choose path (Choisir un chemin).

   c. (Facultatif) Pour Manifest object version ID - optional (ID de version de l'objet manifeste - facultatif), saisissez l'ID de version de l'objet manifeste si vous souhaitez utiliser une autre version que la plus récente.
6. Choisissez Suivant.

7. Pour utiliser la fonction Lambda afin de transcoder tous les objets répertoriés dans le fichier `manifest.json` sélectionné, sous Type d'opération, choisissez Invoquer la fonction AWS Lambda .
8. Dans la section Appeler une fonction Lambda, procédez comme suit :
   a. Choisissez Choisir parmi les fonctions dans votre compte.
   b. Pour Lambda function (Fonction Lambda), choisissez la fonction Lambda que vous avez créée à l'étape 4 (par exemple, **`tutorial-lambda-convert`**).
   c. Pour Lambda function version (Version de la fonction Lambda), conservez la valeur par défaut $LATEST.
9. Choisissez Suivant. La page Configure additional options (Configurer des options supplémentaires) s'ouvre.
10. Dans la section Additional options (Options supplémentaires), conservez les paramètres par défaut.

    Pour plus d'informations sur ces options, consultez Éléments d'une demande de tâche d'opération par lot.
11. Dans la section Rapport d'achèvement, pour Chemin vers la destination du rapport d'achèvement, choisissez Parcourir S3. Recherchez le compartiment que vous avez créé à l'étape 1 pour des fichiers multimédias de sortie (par exemple, *`amzn-s3-demo-destination-bucket1`*). Choisissez le bouton d'option en regard du nom de ce compartiment. Ensuite, choisissez Choose path (Choisir un chemin).

    Pour les paramètres de rapport d'achèvement restants, conservez les paramètres par défaut. Pour en savoir plus sur les paramètres des rapports d'achèvement, consultez Éléments d'une demande de tâche d'opération par lot. Un rapport d'achèvement conserve un enregistrement des détails de la tâche et des opérations exécutées.
12. Dans la section Permissions (Autorisations), choisissez Choose from existing IAM roles (Choisir parmi les rôles IAM existants). Pour Rôle IAM, choisissez le rôle IAM pour votre tâche S3 Batch Operations job que vous avez créée à l'étape 6 (par exemple, **`tutorial-s3batch-role`**).
13. Choisissez Suivant.
14. Sur la page Review (Vérification), vérifiez les paramètres. Ensuite, choisissez Create job (Créer une tâche).

    Lorsque S3 termine la lecture du manifeste de votre tâche S3 Batch Operations, la tâche passe à l'état Awaiting your confirmation to run (En attente de confirmation). Pour afficher les mises à jour

de l'état de la tâche, actualisez la page. Vous ne pouvez pas exécuter votre tâche tant que son statut n'est pas Awaiting your confirmation to run (En attente de confirmation).

Exécutez la tâche d'opérations par lot S3 pour invoquer votre fonction Lambda

Exécutez votre tâche d'opérations par lots pour invoquer votre fonction Lambda aux fins de transcodage vidéo. Si votre tâche échoue, vous pouvez vérifier votre rapport d'achèvement pour identifier la cause.

Pour exécuter la tâche S3 Batch Operations

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Batch Operations (Opérations par lot).
3. Dans la liste Jobs (Tâches), choisissez l'ID de tâche de la tâche sur la première ligne, qui est la tâche S3 Batch Operations que vous avez créée précédemment.
4. Choisissez Exécuter la tâche.
5. Vérifiez à nouveau les paramètres de votre tâche et confirmez que la valeur du Nombre total d'objets répertoriés dans le manifeste est le même que le nombre d'objets indiqué dans le manifeste. Ensuite, choisissez Run job (Exécuter la tâche).

   La page de votre tâche S3 Batch Operations s'ouvre.
6. Lorsque la tâche aura commencé à s'exécuter, dans la page de votre tâche, sous État, vérifiez la progression de votre tâche S3 Batch Operations, par exemple État, % Terminé, Total réussi (débit),Total échoué (débit), Date de la résiliation, et Raison de la résiliation.

   Lorsque la tâche S3 Batch Operations sera terminée, affichez les données dans la page de votre tâche pour confirmer qu'elle s'est achevée comme prévu.

   Si plus de 50 % des opérations objet d'une tâche S3 Batch Operations échouent après que plus de 1 000 opérations aient été tentées, la tâche échouera automatiquement. Pour vérifier votre rapport d'achèvement afin d'identifier la cause des échecs, utilisez la procédure facultative ci-dessous.

(Facultatif) Vérifiez votre rapport d'achèvement

Vous pouvez utiliser votre rapport d'achèvement pour déterminer quels objets ont échoué et la cause des échecs.

Pour vérifier votre rapport d'achèvement afin d'obtenir plus de détails sur les objets qui ont échoué

1. Dans la page de votre tâche S3 Batch Operations, faites défiler jusqu'à la section Completion report (Rapport d'achèvement), puis cliquez sur le lien sous Completion report destination (Destination du rapport d'achèvement).

   La page du compartiment de destination de sortie S3 s'ouvre.
2. Dans l'onglet Objects (Objets), choisissez le dossier dont le nom se termine par l'ID de tâche de la tâche S3 Batch Operations que vous avez créée précédemment.
3. Choisissez résultats/.
4. Cochez la case en regard du fichier `.csv`.
5. Pour afficher le rapport de la tâche, choisissez Open (Ouvrir) ou Download (Télécharger).

(Facultatif) Contrôlez chaque invocation Lambda dans la console Lambda

Lorsque la tâche d'opérations par lot S3 commence à s'exécuter, la tâche invoque la fonction Lambda pour chaque objet d'entrée vidéo. S3 écrit les journaux de chaque appel Lambda dans Logs. CloudWatch Vous pouvez utiliser le tableau de bord de surveillance de la console Lambda pour surveiller votre fonction Lambda.

1. Ouvrez la AWS Lambda console à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le volet de navigation de gauche, choisissez Fonctions.
3. Dans la liste Functions (Fonctions), choisissez le nom de la fonction Lambda que vous avez créée à l'étape 4 (par exemple, **`tutorial-lambda-convert`**).
4. Choisissez l'onglet Surveiller.
5. Sous Métriques, consultez les mesures de l'environnement d'exécution de votre fonction Lambda.
6. Sous Logs, consultez les données du journal pour chaque appel Lambda via CloudWatch Logs Insights.

> **Note**
>
> Si vous utilisez des opérations de lots S3 avec une fonction Lambda, la fonction Lambda sera invoquée sur chaque objet. Si votre tâche d'opérations par lot S3 est volumineuse, elle pourra invoquer plusieurs fonctions Lambda en même temps, provoquant un pic dans la simultanéité Lambda.
> Chacune Compte AWS dispose d'un quota de simultanéité Lambda par région. Pour plus d'informations, consultez AWS Lambda Function Scaling (Mise à l'échelle de fonction Lambda) dans le Guide du développeur AWS Lambda . Une bonne pratique pour utiliser les fonctions Lambda avec les opérations par lots S3 consiste à définir une limite de simultanéité sur la fonction Lambda elle-même. La définition d'une limite de simultanéité empêche votre tâche de consommer la majeure partie de votre simultanéité Lambda et de limiter éventuellement d'autres fonctions de votre compte. Pour plus d'informations, consultez Gestion de la simultanéité réservée Lambda dans le Guide du développeur AWS Lambda .

(Facultatif) Surveillez chaque tâche de MediaConvert transcodage vidéo dans la console MediaConvert

Une MediaConvert tâche consiste à transcoder un fichier multimédia. Lorsque votre tâche S3 Batch Operations appelle votre fonction Lambda pour chaque vidéo, chaque appel de fonction Lambda crée MediaConvert une tâche de transcodage pour chaque vidéo en entrée.

1. Connectez-vous à la MediaConvert console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/mediaconvert/.
2. Si la page MediaConvert d'introduction apparaît, choisissez Commencer.
3. Dans la liste des Tâches, affichez chaque ligne pour contrôler la tâche de transcodage pour chaque vidéo d'entrée.
4. Identifiez la ligne d'une tâche à vérifier, puis cliquez sur le lien Job ID (ID de tâche) pour ouvrir la page de détails de la tâche.
5. Sur la page de résumé du Job, sous Sorties, cliquez sur le lien vers la sortie HLS ou Thumbnails, selon ce qui est pris en charge par votre navigateur, pour accéder au compartiment de destination S3 pour les fichiers multimédia de sortie. MP4
6. Dans le dossier correspondant (HLS ou Thumbnails) de votre compartiment de destination de sortie S3, choisissez le nom de l'objet du fichier multimédia de sortie. MP4

La page de détails de l'objet s'ouvre.

7. Dans la page de détails de l'objet, sous Object overview (Présentation de l'objet), choisissez le lien sous la rubrique Object URL (URL de l'objet) pour regarder le fichier multimédia de sortie transcodé.

Étape 8 : vérifier les fichiers multimédias de sortie à partir de votre compartiment de destination S3

Vérifier les fichiers multimédias de sortie à partir de votre compartiment de destination S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment de destination S3 pour les fichiers multimédias de sortie que vous avez créés à l'étape 1 (par exemple, *amzn-s3-demo-destination-bucket1*).
4. Dans l'onglet Objets, chaque vidéo d'entrée possède un dossier portant le nom de la vidéo d'entrée. Chaque dossier contient les fichiers multimédias de sortie transcodés d'une vidéo d'entrée.

   Pour vérifier les fichiers multimédias de sortie d'une vidéo d'entrée, procédez comme suit :

   a. Choisissez le dossier portant le nom de la vidéo d'entrée que vous souhaitez vérifier.
   b. Choisissez le dossier Par défaut/.
   c. Choisissez le dossier pour un format transcodé (HLS ou miniatures dans ce didacticiel). MP4
   d. Choisissez le nom du fichier multimédia de sortie.
   e. Pour regarder le fichier transcodé, choisissez le lien sous URL de l'objet dans la page de détails de l'objet.

      Les fichiers multimédia de sortie au format HLS sont divisés en segments courts. Pour lire ces vidéos, intégrez l'URL de l'objet du fichier `.m3u8` dans un lecteur compatible.

Étape 9 : nettoyer

Si vous avez transcodé des vidéos à l'aide de S3 Batch Operations, Lambda, MediaConvert et uniquement dans le cadre d'un exercice d'apprentissage, supprimez AWS les ressources que vous avez allouées afin de ne plus payer de frais.

Sous-étapes

- Supprimer la configuration d'inventaire S3 de votre compartiment source S3
- Supprimer la fonction Lambda
- Supprimer le groupe de CloudWatch journaux
- Supprimer les rôles IAM en même temps que les politiques en ligne des rôles IAM
- Supprimer la politique IAM gérée par le client
- Vider les compartiments S3
- Supprimer les compartiments S3

Supprimer la configuration d'inventaire S3 de votre compartiment source S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans Compartiments, choisissez le nom de votre compartiment source (par exemple, *amzn-s3-demo-source-bucket*).
4. Choisissez l'onglet Gestion.
5. Sous Inventory configurations (Configurations d'inventaire), choisissez le bouton radio en regard de la configuration d'inventaire que vous avez créée à l'étape 5 (par exemple, **tutorial-inventory-config**).
6. Choisissez Supprimer, puis choisissez Confirmer.

Supprimer la fonction Lambda

1. Ouvrez la AWS Lambda console à l'adresse https://console.aws.amazon.com/lambda/.
2. Dans le volet de navigation de gauche, choisissez Fonctions.
3. Cochez la case en regard de la fonction que vous avez créée à l'étape 4 (par exemple, **tutorial-lambda-convert**).

4. Choisissez Actions, puis Supprimer.
5. Dans la boîte de dialogue Supprimer une fonction, choisissez Supprimer.

Supprimer le groupe de CloudWatch journaux

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation de gauche, choisissez Journaux, puis Groupes de journaux.
3. Cochez la case en regard du groupe de journaux dont le nom se termine par la fonction Lambda que vous avez créée à l'étape 4 (par exemple, **`tutorial-lambda-convert`**).
4. Choisissez Actions, puis Supprimer le ou les groupes de journaux.
5. Dans la boîte de dialogue Supprimer le ou les groupes de journaux), choisissez Supprimer.

Supprimer les rôles IAM en même temps que les politiques en ligne des rôles IAM

Pour supprimer les rôles IAM que vous avez créés à l'étape 2, à l'étape 3 et à l'étape 6, procédez comme suit :

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation, choisissez Rôles, puis cochez les cases en regard des noms que vous souhaitez supprimer.
3. En haut de la page, choisissez Supprimer.
4. Dans la boîte de dialogue de confirmation, saisissez la réponse requise dans la zone de saisie de texte en fonction de l'invite, puis choisissez Supprimer.

Supprimer la politique IAM gérée par le client

Pour supprimer la politique IAM gérée par le client que vous avez créée à l'étape 6, procédez comme suit :

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation de gauche, choisissez Politiques.

3. Choisissez le bouton radio en regard de la stratégie que vous avez créée à l'étape 6 (par exemple, **`tutorial-s3batch-policy`**). Vous pouvez utiliser la zone de recherche pour filtrer la liste des politiques.
4. Choisissez Actions, puis choisissez Supprimer.
5. Confirmez que vous souhaitez supprimer cette stratégie en saisissant son nom dans le champ de texte, puis choisissez Delete (Supprimer).

Vider les compartiments S3

Pour vider les compartiments S3 que vous avez créés dans Prerequisites (Prérequis), à l'étape 1 et à l'étape 5, procédez comme suit :

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le bouton radio en regard du nom du compartiment à vider, puis choisissez Empty (Vider).
4. Dans la page Empty bucket (Vider le compartiment), confirmez que vous souhaitez vider le compartiment en saisissant **`permanently delete`** dans le champ de texte, puis choisissez Empty (Vider).

Supprimer les compartiments S3

Pour supprimer les compartiments S3 que vous avez créés dans Prerequisites (Prérequis), à l'étape 1 et à l'étape 5, procédez comme suit :

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le bouton radio en regard du nom du compartiment que vous souhaitez supprimer.
4. Choisissez Supprimer.
5. Dans la page Supprimer le compartiment, confirmez que vous souhaitez supprimer le compartiment en saisissant le nom de ce dernier dans le champ de texte, puis choisissez Supprimer le compartiment.

Étapes suivantes

Après avoir terminé ce didacticiel, vous pourrez explorer d'autres cas d'utilisation pertinents :

- Vous pouvez utiliser Amazon CloudFront pour diffuser les fichiers multimédia transcodés aux spectateurs du monde entier. Pour de plus amples informations, veuillez consulter Tutoriel : Hébergement de vidéos en streaming à la demande avec Amazon S3 CloudFront, Amazon et Amazon Route 53.
- Vous pouvez transcoder des vidéos au moment où vous les téléchargez dans le compartiment source S3. Pour ce faire, vous pouvez configurer un déclencheur d'événement Amazon S3 qui invoque automatiquement la fonction Lambda pour transcoder de nouveaux objets dans S3 avec. MediaConvert Pour plus d'informations, consultez Didacticiels : Utilisation d'un déclencheur Amazon S3 pour invoquer une fonction Lambda dans le Guide du développeur AWS Lambda .

Résolution des problèmes d'opérations par lot

Les rubriques suivantes traitent des erreurs courantes afin de vous aider à résoudre les problèmes que vous pourriez rencontrer lors de l'utilisation d'Amazon S3 Batch Operations.

Pour résoudre les problèmes liés à la réplication par lot S3, consultez the section called "Erreurs de réplication par lot".

Il existe deux principaux types de défaillances qui entraînent des erreurs de fonctionnement du mode Batch :

- Échec de l'API — L'API demandée (telle que`CreateJob`) n'a pas pu être exécutée.
- Échec de la tâche : la demande d'API initiale a réussi, mais la tâche a échoué, par exemple en raison de problèmes liés au manifeste ou aux autorisations d'accès aux objets spécifiés dans le manifeste.

NoSuchJobException

Type : échec de l'API

Cela peut se produire si la tâche a expiré ou lorsque l'identifiant utilisé dans la `CreateJob` demande n'est pas le même que celui utilisé dans la `UpdateJobStatus` demande `DescribeJob` ou.

Les jobs expirent après 90 jours dans un état terminal (`Complete`,`Cancelled`, ou`Failed`) Pour plus d'informations, consultezthe section called "Suivi de l'état de la tâche et des rapports de fin de tâche".

Messages d'erreur associés

`No such job`

Actions recommandées

Pour résoudre le problème, `NoSuchJobException` vous pouvez essayer ce qui suit :

1. Vérifiez que l'offre d'emploi existe et se trouve dans votre compte. Vous pouvez utiliser la AWS CLI commande suivante : `aws s3control list-jobs --account-id 111122223333`
2. Vérifiez que l'identifiant reçu dans la `CreateJob` demande est le même que celui utilisé dans la `UpdateJobStatus` demande `DescribeJob` ou.

AccessDeniedException

Type : échec de l'API

Cela se `AccessDeniedException` produit lorsqu'une demande S3 Batch Operations est bloquée en raison d'opérations non prises en charge ou lorsque l'identité IAM à l'origine de la demande ne dispose pas des autorisations suffisantes pour effectuer une action.

Messages d'erreur associés

`Access Denied`

Actions recommandées

Pour résoudre le problème, AccessDeniedException vous pouvez essayer ce qui suit :

1. Assurez-vous que S3 Batch Operations prend en charge l'opération ou la fonctionnalité dans la région. Pour une liste des opérations prises en charge, consultez the section called “Opérations prises en charge”. Les opérations par lots sont prises en charge pour les compartiments à usage général dans toutes les régions, mais les opérations pour les compartiments de répertoire ne sont disponibles que dans les points de terminaison régionaux et zonaux pour les compartiments de répertoire.
2. Assurez-vous que l'identité IAM à l'origine de la demande est autorisée à créer et à gérer des opérations par lots. Pour obtenir la liste des autorisations, voirthe section called “Octroi d'autorisations”.

SlowDownError

Type : échec de l'API

L'`SlowDownError`exception se produit lorsque votre compte a dépassé la limite de taux de demandes pour S3 Batch Operations.

Actions recommandées

Pour résoudre les `SlowDownError` exceptions, vous pouvez essayer ce qui suit :

1. Ralentissez le taux de demandes et réessayez. Pour plus d'informations, voir Réessayer avec un schéma d'interruption dans les directives AWS prescriptives.

InvalidManifestContent

Type : Échec du Job

L'`InvalidManifestContent`exception se produit en cas de problèmes liés au format du fichier manifeste ou au contenu utilisé par S3 Batch Operations pour traiter les objets.

Messages d'erreur associés

- `Required fields are missing in the schema: + missingFields`
- `Invalid Manifest Content`
- `The S3 Batch Operations job failed because it contains more keys than the maximum allowed in a single job. Please split the job into multiple smaller jobs or reach out to customer support for next steps.`

Actions recommandées

Pour résoudre le problème, `InvalidManifestContent` vous pouvez essayer ce qui suit :

Pour les problèmes liés au format du manifeste :

1. Assurez-vous que le manifeste respecte les spécifications de format requises. Toutes les colonnes requises doivent être présentes, correctement formatées et cohérentes dans l'ensemble du manifeste. Pour obtenir des exemples, consultez the section called “Spécification d'un manifeste”.

Pour les problèmes de contenu :

1. Remplacez les caractères spéciaux des clés d'objet par leurs codes d'entité XML et assurez-vous que les clés d'objet respectent les conventions de dénomination Amazon S3. Pour de plus amples informations, veuillez consulter the section called “Attribution d'un nom aux objets”.
2. Assurez-vous que toutes les clés d'objet sont codées en URL.
3. Divisez les gros travaux en petits travaux. Vous pouvez voir combien d'objets sont pris en charge pour chaque opérationthe section called “Opérations prises en charge”.

Interrogation des données sur place avec Amazon S3 Select

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Avec Amazon S3 Select, vous pouvez utiliser des instructions de langage de requête structurée (SQL) pour filtrer le contenu d'un objet Amazon S3 afin de récupérer uniquement le sous-ensemble de données dont vous avez besoin. En utilisant Amazon S3 Select pour filtrer ces données, vous pouvez réduire la quantité de données transférées par Amazon S3, ce qui limite le coût et la latence de récupération de ces données.

Amazon S3 Select ne vous permet d'interroger qu'un seul objet à la fois. Il fonctionne avec un objet stocké au format CSV, JSON ou Apache Parquet. Il fonctionne également avec un objet compressé avec GZIP ou BZIP2 (pour les objets CSV et JSON uniquement) et un objet chiffré côté serveur. Vous pouvez spécifier les résultats au format CSV ou JSON et vous pouvez décider de la manière dont les enregistrements sont délimités dans le résultat.

Vous transmettez des expression SQL à Amazon S3 dans la demande. Amazon S3 Select prend en charge un sous-ensemble du langage SQL. Pour de plus amples informations sur les éléments SQL pris en charge par Amazon S3 Select, consultez Référence SQL pour Amazon S3 Select.

Vous pouvez effectuer des requêtes SQL à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'opération d'`SelectObjectContent`API REST ou du AWS SDKs.

> **Note**
>
> La console Amazon S3 limite la quantité de données renvoyées à 40 Mo. Pour récupérer davantage de données, utilisez l'API AWS CLI ou.

Exigences et limites

Les exigences pour l'utilisation d'Amazon S3 Select sont les suivantes :

- Vous devez bénéficier d'une autorisation `s3:GetObject` sur le l'objet que vous interrogez.
- Si l'objet que vous interrogez est doté d'un chiffrement côté serveur avec des clés fournies par le client (SSE-C), vous devez utiliser `https` et fournir la clé de chiffrement dans la demande.

Les limites suivantes s'appliquent lors de l'utilisation d'Amazon S3 Select :

- S3 Select ne peut interroger qu'un seul objet par demande.
- La longueur maximale d'une expression SQL est de 256 Ko.
- La longueur maximale d'un enregistrement dans l'entrée ou le résultat est de 1 Mo.
- Amazon S3 Select peut seulement émettre des données imbriquées à l'aide du format de sortie JSON.
- Vous ne pouvez pas interroger un objet stocké dans les classes de stockage S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive ou Reduced Redundancy Storage (RRS). Vous ne pouvez pas non plus interroger un objet stocké dans le niveau d'accès aux archives S3 Intelligent-Tiering ou le niveau d'accès Deep Archive de S3 Intelligent-Tiering. Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

Des limites supplémentaires s'imposent lorsque Amazon S3 Select est utilisé avec un objet Parquet :

- Amazon S3 Select prend en charge uniquement la compression en colonnes avec GZIP ou Snappy. Amazon S3 Select ne prend pas en charge la compression d'objet entier pour les objets Parquet.
- Amazon S3 Select ne prend pas en charge la sortie Parquet. Vous devez spécifier le format de sortie CSV ou JSON.
- La taille maximale des groupes de rangées non compressés est de 512 Mo.

- Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
- Une sélection opérée dans un champ répété renvoie uniquement la dernière valeur.

Création d'une demande

Lorsque vous créez une demande, vous fournissez des informations détaillées sur l'objet interrogé à l'aide d'un objet `InputSerialization`. Vous fournissez des informations détaillées sur la manière dont les résultats doivent être retournés à l'aide d'un objet `OutputSerialization`. Vous incluez également l'expression SQL qu'Amazon S3 Select utilise pour filtrer la demande.

Pour plus d'informations sur la création d'une demande Amazon S3 Select, consultez SelectObjectContent dans la Référence d'API Amazon Simple Storage Service. Vous pouvez également consulter l'un des exemples de code SDK dans les sections suivantes.

Demandes utilisant des plages d'analyse

Amazon S3 Select vous permet d'analyser un sous-ensemble d'un objet en spécifiant une plage d'octets à interroger. Vous pouvez ainsi paralléliser l'analyse de l'objet entier en divisant la tâche en demandes Amazon S3 Select distinctes pour une série de plages d'analyse qui ne se chevauchent pas.

Les plages d'analyse n'ont pas besoin d'être alignées sur des limites d'enregistrement. Une demande de plage d'analyse Amazon S3 Select s'exécute sur la plage d'octets que vous spécifiez. Un enregistrement qui commence dans la plage d'analyse spécifiée mais qui s'étend au-delà de celle-ci est traité par la requête. Par exemple, la section suivante montre un objet Amazon S3 contenant une série d'enregistrements au format CSV délimité par des lignes :

```
A,B
C,D
D,E
E,F
G,H
I,J
```

Supposons que vous utilisiez le paramètre `ScanRange` d'Amazon S3 Select avec Début à (l'octet) 1 et Fin à (l'octet) 4. La plage d'analyse commence donc à « `,` » et l'analyse est exécutée jusqu'à la fin de l'enregistrement, à partir de `C`. Votre demande de plage d'analyse renverra le résultat `C, D` car c'est la fin de l'enregistrement.

Les demandes de plage d'analyse Amazon S3 Select prennent en charge les objets Parquet, CSV (sans délimiteurs entre guillemets) ou JSON (en mode `LINES` uniquement). Les objets CSV et JSON doivent être non compressés. Pour les objets JSON et CSV de type ligne, quand une plage d'analyse est spécifiée dans le cadre d'une demande Amazon S3 Select, tous les enregistrements qui commencent dans la plage d'analyse sont traités. Pour les objets Parquet, tous les groupes de lignes qui commencent dans la plage d'analyse sont traités.

Les demandes de plage de numérisation Amazon S3 Select peuvent être utilisées avec l' AWS CLI API Amazon S3 et AWS SDKs. Vous pouvez utiliser le paramètre `ScanRange` dans la demande Amazon S3 Select pour cette fonction. Pour plus d'informations, consultez SelectObjectContent dans la Référence d'API Amazon Simple Storage Service.

Erreurs

Amazon S3 Select renvoie un code d'erreur et un message d'erreur associé en cas de problème lors de la tentative d'exécution d'une requête. Pour obtenir la liste des codes d'erreur et des descriptions, consultez la section Liste des codes d'erreur SELECT Object Content de la page Réponses d'erreur dans la Référence de l'API Amazon Simple Storage Service.

Pour plus d'informations sur Amazon S3 Select, consultez les rubriques suivantes.

Rubriques

- Exemples d'utilisation d'Amazon S3 Select au niveau d'un objet
- Référence SQL pour Amazon S3 Select

Exemples d'utilisation d'Amazon S3 Select au niveau d'un objet

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Vous pouvez utiliser S3 Select pour sélectionner le contenu d'un objet à l'aide de la console Amazon S3, de l'API REST et du AWS SDKs.

Pour plus d'informations sur les fonctions SQL prises en charge pour S3 Select, consultez Fonctions SQL.

Utilisation de la console S3

Pour sélectionner du contenu à partir d'un objet dans la console Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Choisissez le compartiment qui contient l'objet dont vous souhaitez sélectionner le contenu, puis choisissez le nom de l'objet.
4. Choisissez Actions d'objet, puis Requête avec S3 Select.
5. Configurez Paramètres d'entrée en fonction du format de vos données d'entrée.
6. Configurez Paramètres de sortie en fonction du format de sortie que vous souhaitez recevoir.
7. Pour extraire des enregistrements de l'objet choisi, sous Requête SQL, saisissez les commandes SELECT et SQL. Pour plus d'informations sur la procédure d'écriture de commandes SQL, consultez Référence SQL pour Amazon S3 Select.
8. Après avoir saisi des requêtes SQL, choisissez Exécuter la requête SQL. Ensuite, sous Résultats de la requête, vous pouvez voir les résultats de vos requêtes SQL.

Utilisation de l'API REST

Vous pouvez utiliser le AWS SDKs pour sélectionner le contenu d'un objet. Toutefois, si l'application l'exige, vous pouvez envoyer directement des demandes REST. Pour plus d'informations sur le format de demande et de réponse, consultez SelectObjectContent.

À l'aide du AWS SDKs

Vous pouvez utiliser Amazon S3 Select pour sélectionner une partie du contenu d'un objet à l'aide de la méthode `selectObjectContent`. Si cette méthode aboutit, elle renvoie les résultats de l'expression SQL.

Java

Le code Java suivant retourne la valeur de la première colonne de chaque enregistrement stocké dans un objet contenant les données stockées au format CSV. Il demande également que les

messages `Progress` et `Stats` soient retournés. Vous devez fournir un nom de compartiment valide, ainsi qu'un objet contenant les donnes au format CSV.

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
package com.amazonaws;

import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CSVInput;
import com.amazonaws.services.s3.model.CSVOutput;
import com.amazonaws.services.s3.model.CompressionType;
import com.amazonaws.services.s3.model.ExpressionType;
import com.amazonaws.services.s3.model.InputSerialization;
import com.amazonaws.services.s3.model.OutputSerialization;
import com.amazonaws.services.s3.model.SelectObjectContentEvent;
import com.amazonaws.services.s3.model.SelectObjectContentEventVisitor;
import com.amazonaws.services.s3.model.SelectObjectContentRequest;
import com.amazonaws.services.s3.model.SelectObjectContentResult;

import java.io.File;
import java.io.FileOutputStream;
import java.io.InputStream;
import java.io.OutputStream;
import java.util.concurrent.atomic.AtomicBoolean;

import static com.amazonaws.util.IOUtils.copy;

/**
 * This example shows how to query data from S3Select and consume the response in
 the form of an
 * InputStream of records and write it to a file.
 */

public class RecordInputStreamExample {

    private static final String BUCKET_NAME = "${my-s3-bucket}";
    private static final String CSV_OBJECT_KEY = "${my-csv-object-key}";
    private static final String S3_SELECT_RESULTS_PATH = "${my-s3-select-results-
path}";
    private static final String QUERY = "select s._1 from S3Object s";
```

```
   public static void main(String[] args) throws Exception {
       final AmazonS3 s3Client = AmazonS3ClientBuilder.defaultClient();

       SelectObjectContentRequest request = generateBaseCSVRequest(BUCKET_NAME,
CSV_OBJECT_KEY, QUERY);
       final AtomicBoolean isResultComplete = new AtomicBoolean(false);

       try (OutputStream fileOutputStream = new FileOutputStream(new File
(S3_SELECT_RESULTS_PATH));
            SelectObjectContentResult result =
s3Client.selectObjectContent(request)) {
           InputStream resultInputStream =
result.getPayload().getRecordsInputStream(
                   new SelectObjectContentEventVisitor() {
                       @Override
                       public void visit(SelectObjectContentEvent.StatsEvent event)
                       {
                           System.out.println(
                                   "Received Stats, Bytes Scanned: " +
event.getDetails().getBytesScanned()
                                           +  " Bytes Processed: " +
event.getDetails().getBytesProcessed());
                       }

                       /*
                        * An End Event informs that the request has finished
successfully.
                        */
                       @Override
                       public void visit(SelectObjectContentEvent.EndEvent event)
                       {
                           isResultComplete.set(true);
                           System.out.println("Received End Event. Result is
complete.");
                       }
                   }
           );

           copy(resultInputStream, fileOutputStream);
       }

       /*
        * The End Event indicates all matching records have been transmitted.
        * If the End Event is not received, the results may be incomplete.
```

```
             */
            if (!isResultComplete.get()) {
                throw new Exception("S3 Select request was incomplete as End Event was
     not received.");
            }
        }

        private static SelectObjectContentRequest generateBaseCSVRequest(String bucket,
     String key, String query) {
            SelectObjectContentRequest request = new SelectObjectContentRequest();
            request.setBucketName(bucket);
            request.setKey(key);
            request.setExpression(query);
            request.setExpressionType(ExpressionType.SQL);

            InputSerialization inputSerialization = new InputSerialization();
            inputSerialization.setCsv(new CSVInput());
            inputSerialization.setCompressionType(CompressionType.NONE);
            request.setInputSerialization(inputSerialization);

            OutputSerialization outputSerialization = new OutputSerialization();
            outputSerialization.setCsv(new CSVOutput());
            request.setOutputSerialization(outputSerialization);

            return request;
        }
    }
```

JavaScript

Pour un JavaScript exemple d'utilisation de l'opération AWS SDK pour JavaScript avec l'`SelectObjectContent`API S3 pour sélectionner des enregistrements à partir de fichiers JSON et CSV stockés dans Amazon S3, consultez le billet de blog Présentation de la prise en charge d'Amazon S3 Select dans le AWS SDK pour JavaScript.

Python

Pour un exemple Python sur l'utilisation de requêtes SQL pour effectuer des recherches dans des données chargées sur Amazon S3 en tant que fichier CSV (valeur séparée par des virgules) à l'aide de S3 Select, consultez le billet de blog Interrogation de données sans serveur ou base de données à l'aide d'Amazon S3 Select.

Référence SQL pour Amazon S3 Select

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Cette référence contient une description des éléments du langage de recherche structurée (SQL) pris en charge par Amazon S3 Select.

Rubriques

- SELECT commande
- Types de données
- Opérateurs
- Mots-clés réservés
- Fonctions SQL

SELECT commande

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge uniquement la commande SQL `SELECT`. Les clauses standard ANSI suivantes sont prises en charge pour `SELECT` :

- `SELECT` liste
- `FROM`Clause
- `WHERE`Clause
- `LIMIT`Clause

> **Note**
>
> Les requêtes Amazon S3 Select ne prennent actuellement pas en charge les sous-requêtes ni les jointures.

SELECT liste

La liste SELECT nomme les colonnes, fonctions et expressions que la requête doit renvoyer. La liste représente le résultat de la requête.

```
SELECT *
SELECT projection1 AS column_alias_1, projection2 AS column_alias_2
```

Le premier format SELECT avec * (astérisque) renvoie chaque ligne ayant transmis la clause WHERE, telle qu'elle. Le second format SELECT crée une ligne avec la ***projection1*** et la ***projection2*** des expressions scalaires de sortie définies par l'utilisateur de chaque colonne.

FROMClause

Amazon S3 Select prend en charge les formes suivantes de la clause FROM :

```
FROM table_name
FROM table_name alias
FROM table_name AS alias
```

Dans chaque forme de la clause FROM, `table_name` est le `S3Object` qui est interrogé. Les utilisateurs provenant de bases de données relationnelles traditionnelles peuvent penser qu'il s'agit d'un schéma de base de données contenant plusieurs vues sur une table.

Dans le langage SQL standard, la clause FROM crée des lignes qui sont filtrées dans la clause WHERE et projetées dans la liste SELECT.

Pour les objets JSON stockés dans Amazon S3 Select, vous pouvez également utiliser les formes suivantes de la clause FROM :

```
FROM S3Object[*].path
FROM S3Object[*].path alias
FROM S3Object[*].path AS alias
```

En utilisant cette forme de la clause FROM, vous pouvez effectuer une sélection dans les tableaux ou les objets contenus dans un objet JSON. Vous pouvez spécifier `path` en utilisant l'un des formats suivants :

- Par nom (dans un objet) : `.name` ou `['name']`
- Par index (dans un tableau)) : `[index]`
- Par caractère générique (dans un objet) : `.*`
- Par caractère générique (dans un tableau) : `[*]`

> **Note**
>
> - Cette forme de la clause FROM fonctionne uniquement avec les objets JSON.
> - Les caractères génériques émettent toujours au moins un enregistrement. Si aucun enregistrement ne correspond, Amazon S3 Select émet la valeur MISSING. Pendant la sérialisation de la sortie (après que la requête a fini de s'exécuter), Amazon S3 Select remplace les valeurs MISSING par des enregistrements vides.
> - Les fonctions d'agrégation (AVG, COUNT, MAX, MIN et SUM) ignorent les valeurs MISSING.
> - Si, lorsque vous utilisez un caractère générique, vous n'indiquez pas d'alias, vous pouvez faire référence à la ligne en utilisant le dernier élément du chemin. Par exemple, vous pouvez sélectionner tous les prix d'une liste de livres en utilisant la requête `SELECT price FROM S3Object[*].books[*].price`. Si le chemin se termine par un caractère générique plutôt qu'un nom, vous pouvez utiliser la valeur `_1` pour faire référence à la ligne. Par exemple, à la place de `SELECT price FROM S3Object[*].books[*].price`, vous pouvez utiliser la requête `SELECT _1.price FROM S3Object[*].books[*]`.
> - Amazon S3 Select traite toujours un document JSON comme un tableau de valeurs de niveau racine. Par conséquent, même si l'objet JSON que vous interrogez ne contient qu'un seul élément racine, la clause FROM doit commencer par `S3Object[*]`. Toutefois, pour des raisons de compatibilité, Amazon S3 Select vous autorise à omettre le caractère générique si vous n'incluez pas de chemin. Ainsi, la clause complète `FROM S3Object` équivaut à `FROM S3Object[*] as S3Object`. Si vous incluez un chemin, vous devez également utiliser le caractère générique. Autrement dit, `FROM S3Object` et `FROM S3Object[*].path` sont deux clauses valides, mais pas `FROM S3Object.path`.

Example

Exemples :

Exemple 1

Cet exemple affiche les résultats quand le jeu de données et la requête suivants sont utilisés :

```
{ "Rules": [ {"id": "1"}, {"expr": "y > x"}, {"id": "2", "expr": "z = DEBUG"} ]}
{ "created": "June 27", "modified": "July 6" }
```

```
SELECT id FROM S3Object[*].Rules[*].id
```

```
{"id":"1"}
{}
{"id":"2"}
{}
```

Amazon S3 Select génère chaque résultat pour les raisons suivantes :

- `{"id":"id-1"}` : `S3Object[0].Rules[0].id` a produit une correspondance.
- `{}` : `S3Object[0].Rules[1].id` n'a pas produit de correspondance. Amazon S3 Select a donc émis `MISSING`, qui a ensuite été changé en enregistrement vide pendant la sérialisation de la sortie avant d'être renvoyé.
- `{"id":"id-2"}` : `S3Object[0].Rules[2].id` a produit une correspondance.
- `{}` : `S3Object[1]` n'a pas produit de correspondance sur `Rules`. Amazon S3 Select a donc émis `MISSING`, qui a ensuite été changé en enregistrement vide pendant la sérialisation de la sortie avant d'être renvoyé.

Si vous ne voulez pas qu'Amazon S3 Select renvoie des enregistrements vides en l'absence de correspondance, vous pouvez faire un test avec la valeur `MISSING`. La requête suivante renvoie les mêmes résultats que la requête précédente, à la différence près que les valeurs vides sont omises :

```
SELECT id FROM S3Object[*].Rules[*].id WHERE id IS NOT MISSING
```

```
{"id":"1"}
{"id":"2"}
```

Exemple 2

Cet exemple affiche les résultats quand le jeu de données et les requêtes suivants sont utilisés :

```
{ "created": "936864000", "dir_name": "important_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": ".aws" }, { "name": "downloads" } ], "owner": "Amazon
 S3" }
{ "created": "936864000", "dir_name": "other_docs", "files": [ { "name": "." },
 { "name": ".." }, { "name": "my stuff" }, { "name": "backup" } ], "owner": "User" }
```

```
SELECT d.dir_name, d.files FROM S3Object[*] d
```

```
{"dir_name":"important_docs","files":[{"name":"."},{"name":".."},{"name":".aws"},
{"name":"downloads"}]}
{"dir_name":"other_docs","files":[{"name":"."},{"name":".."},{"name":"my stuff"},
{"name":"backup"}]}
```

```
SELECT _1.dir_name, _1.owner FROM S3Object[*]
```

```
{"dir_name":"important_docs","owner":"Amazon S3"}
{"dir_name":"other_docs","owner":"User"}
```

WHEREClause

La clause `WHERE` suit la syntaxe suivante :

```
WHERE condition
```

La clause `WHERE` filtre les lignes en fonction de la *`condition`*. Une condition est une expression générant un résultat booléen. Seules les lignes pour lesquelles la condition a la valeur `TRUE` sont renvoyées dans les résultats.

LIMITClause

La clause `LIMIT` suit la syntaxe suivante :

```
LIMIT number
```

La clause `LIMIT` limite le nombre d'enregistrements que la requête devra renvoyer en fonction du *`number`*.

Accès aux attributs

Les clauses `SELECT` et `WHERE` peuvent faire référence à des enregistrements à l'aide d'une des méthodes présentées dans les sections suivantes, la méthode utilisée variant selon le format du fichier interrogé (CSV ou JSON).

CSV

- Numéros de colonne : vous pouvez faire référence à la Nième colonne d'une ligne avec un nom de colonne *_N*, où *N* correspond à la position de la colonne. Le compte de la position commence à 1. Par exemple, la première colonne est appelée _1 et la deuxième colonne est appelée _2.

  Vous pouvez faire référence à une colonne sous la forme *_N* ou *alias*.*_N*. Par exemple, _2 et `myAlias._2` sont deux manières valides de faire référence à une colonne de la liste `SELECT` et la clause `WHERE`.
- En-têtes de colonne – Concernant les objets au format CSV ayant une ligne d'en-tête, les en-têtes sont disponibles pour la liste `SELECT` et la clause `WHERE`. Comme dans le SQL traditionnel, dans les expressions de clause `SELECT` et `WHERE`, vous pouvez faire référence aux colonnes via *alias*.*column_name* ou *column_name*.

JSON

- Document – Vous pouvez accéder aux champs du document JSON sous la forme *alias*.*name*. Vous pouvez aussi accéder au champs imbriqués ; par exemple, *alias*.*name1*.*name2*.*name3*.
- Liste : vous pouvez accéder aux éléments d'une liste JSON en utilisant des index de base zéro avec l'opérateur `[]`. Par exemple, vous pouvez accéder au second élément d'une liste sous la forme *alias*`[1]`. Vous pouvez combiner l'accès aux éléments de la liste avec des champs, par exemple, *alias*.*name1*.*name2*`[1]`.*name3*.
- Exemples : Considérez cet objet JSON comme un exemple de jeu de données :

```
{"name": "Susan Smith",
"org": "engineering",
"projects":
    [
     {"project_name":"project1", "completed":false},
     {"project_name":"project2", "completed":true}
    ]
}
```

Exemple 1

La requête suivante renvoie ces résultats :

```
Select s.name from S3Object s
```

```
{"name":"Susan Smith"}
```

Exemple 2

La requête suivante renvoie ces résultats :

```
Select s.projects[0].project_name from S3Object s
```

```
{"project_name":"project1"}
```

Sensibilité à la casse des noms d'en-tête et d'attribut

Avec Amazon S3 Select, vous pouvez utiliser des guillemets doubles pour indiquer que les en-têtes de colonne (pour les objets CSV) et les attributs (pour les objets JSON) sont sensibles à la casse. Sans guillemets doubles, les en-têtes et les attributs d'objet sont sensibles à la casse. Une erreur est envoyée en cas d'ambiguïté.

Les exemples suivants sont 1) des objets Amazon S3 au format CSV avec les en-têtes de colonne spécifiés et avec `FileHeaderInfo` défini sur `"Use"` pour la demande de requête ou 2) des objets Amazon S3 au format JSON avec les attributs spécifiés.

Exemple n°1 : l'objet interrogé possède l'en-tête ou l'attribut `NAME`.

- L'expression suivante renvoie avec succès les valeurs de l'objet. Comme il n'y a pas de guillemets, la requête est sensible à la casse.

  ```
  SELECT s.name from S3Object s
  ```

- L'expression suivante renvoie une erreur 400 `MissingHeaderName`. Comme il y a des guillemets, la requête est sensible à la casse.

```
SELECT s."name" from S3Object s
```

Exemple n°2 : l'objet Amazon S3 interrogé possède un en-tête ou un attribut avec `NAME` et un autre en-tête ou attribut avec `name`.

- L'expression suivante renvoie une erreur 400 `AmbiguousFieldName`. Comme il n'y a pas de guillemets doubles, la requête est sensible à la casse, mais il y a deux correspondances : l'erreur est renvoyée.

  ```
  SELECT s.name from S3Object s
  ```

- L'expression suivante renvoie avec succès les valeurs de l'objet. Comme il y a des guillemets, la requête est sensible à la casse sans qu'il y ait d'ambiguïté.

  ```
  SELECT s."NAME" from S3Object s
  ```

Utilisation de mots-clés réservés comme termes définis par l'utilisateur

Amazon S3 Select dispose d'un ensemble de mots-clés réservés nécessaires pour exécuter les expressions SQL utilisées pour interroger le contenu d'un objet. Les mots-clés réservés peuvent être des noms de fonctions, des types de données, des opérateurs, etc. Dans certains cas, les termes définis par l'utilisateur comme les en-têtes de colonnes (pour les fichiers CSV) ou les attributs (pour les objets JSON) peuvent entrer en conflit avec un mot-clé réservé. Lorsque cela se produit, vous devez utiliser des guillemets doubles pour indiquer que vous utilisez intentionnellement un terme défini par l'utilisateur qui est en conflit avec un mot-clé réservé. Si vous ne le faites pas, un erreur d'analyse 400 est émise.

Pour obtenir la liste complète des mots-clés réservés, consultez Mots-clés réservés.

L'exemple suivant est 1) un objet Amazon S3 au format CSV avec les en-têtes de colonne spécifiés et avec `FileHeaderInfo` défini sur `"Use"` pour la demande de requête ou 2) un objet Amazon S3 au format JSON avec les attributs spécifiés.

Exemple : l'objet interrogé possède un en-tête ou un attribut `CAST`, qui est un mot-clé réservé.

- L'expression suivante renvoie avec succès les valeurs de l'objet. Comme les guillemets sont utilisés dans la requête, S3 Select utilise l'en-tête ou l'attribut défini par l'utilisateur.

```
SELECT s."CAST" from S3Object s
```

- L'expression suivante renvoie une erreur d'analyse 400. Comme aucun guillemet n'est utilisé dans la requête, CAST entre en conflit avec un mot-clé réservé.

```
SELECT s.CAST from S3Object s
```

Expressions scalaires

Au sein de la clause WHERE et de la liste SELECT, vous pouvez disposez d'expressions scalaires SQL, qui sont des expressions qui renvoient des valeurs scalaires. Elles sont au format suivant :

- ***literal***

  Littéral SQL.

- ***column_reference***

  Référence à une colonne au format *column_name* ou *alias*.*column_name*.

- ***unary_op expression***

  Dans ce cas, ***unary_op*** est un opérateur unaire SQL.

- ***expression binary_op expression***

  Dans ce cas, ***binary_op*** est un opérateur binaire SQL.

- ***func_name***

  Dans ce cas, ***func_name*** est le nom de la fonction scalaire à invoquer.

- ***expression*** [NOT] BETWEEN ***expression*** AND ***expression***
- ***expression*** LIKE ***expression*** [ESCAPE ***expression***]

Types de données

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge plusieurs types de données primitifs.

Conversions du type de données

La règle générale consiste à suivre la fonction `CAST` si elle est définie. Si `CAST` n'est pas défini, toutes les données d'entrée sont considérées comme une chaîne. Dans ce cas, vous devez convertir vos données d'entrée dans les types de données concernés au besoin.

Pour plus d'informations sur la fonction `CAST`, consultez CAST.

Types de données pris en charge

Amazon S3 Select prend en charge l'ensemble de types de données primitifs suivant.

Name (Nom)	Description	Exemples
`bool`	Une valeur booléenne, `TRUE` ou `FALSE`.	`FALSE`
`int`, `integer`	Un entier signé sur 8 octets dans la plage -9 223 372 036 854 775 808 à 9 223 372 036 854 775 807.	`100000`
`string`	Chaîne de UTF8 longueur variable codée. La limite par défaut est de un caractère. La limite de caractères maximale est de 2 147 483 647.	`'xyz'`
`float`	Un nombre à virgule flottante de 8 octets.	`CAST(0.456 AS FLOAT)`
`decimal`, `numeric`		`123.456`

Name (Nom)	Description	Exemples
	Un nombre de base 10, avec une précision maximale de 38 (c'est-à-dire, le nombre maximal de chiffres significatifs) et avec une échelle dans la plage de -2^{31} à $2^{31}-1$ (c'est-à-dire, l'exposant de base 10). **Note** Amazon S3 Select ignore l'échelle et la précision lorsque vous fournissez les deux en même temps.	
`timestamp`	Les horodatages représentent un moment spécifique dans le temps, incluent toujours un décalage local, et sont capables de précision arbitraire. Dans le format de texte, les horodatages suivent la remarque de W3C sur les formats de date et d'heure, mais ils doivent se terminer par le `T` littéral si la précision des horodatages n'est pas d'une journée complète. Les fractions de seconde sont autorisées, avec une précision d'au moins un chiffre et un maximum illimité. Les décalages en heure locale peuvent être représentés sous forme de décalages heure:minute en UTC, ou en tant que `Z` littéral pour indiquer une heure locale en UTC. Les décalages en heure locale sont obligatoires sur les horodatages incluant l'heure et ne sont pas autorisés sur les valeurs de date.	`CAST('2007-04-05T14:30Z' AS TIMESTAMP)`

Types Parquet pris en charge

Amazon S3 Select prend en charge les types Parquet suivants.

- `DATE`
- `DECIMAL`
- `ENUM`
- `INT(8)`

- INT(16)
- INT(32)
- INT(64)
- LIST

> **Note**
>
> Pour les sorties de type LIST Parquet, Amazon S3 Select ne prend en charge que le format JSON. Cependant, si la requête limite les données à des valeurs simples, le type LIST Parquet peut également être interrogé au format CSV.

- STRING
- Précision prise en charge par TIMESTAMP (MILLIS/MICROS/NANOS)

> **Note**
>
> Les horodatages enregistrés au format INT(96) ne sont pas pris en charge.
> En raison de la plage du type INT(64), les horodatages utilisant l'unité NANOS ne peuvent représenter que des valeurs comprises entre 1677-09-21 00:12:43 et 2262-04-11 23:47:16. Les valeurs en dehors de cette plage ne peuvent pas être représentées par l'unité NANOS.

Mappage des types Parquet aux types de données pris en charge dans Amazon S3 Select

Types Parquet	Types de données pris en charge
DATE	timestamp
DECIMAL	decimal, numeric
ENUM	string
INT(8)	int, integer

Types Parquet	Types de données pris en charge
INT(16)	int, integer
INT(32)	int, integer
INT(64)	decimal, numeric
LIST	Chaque type Parquet de la liste est mappé au type de données correspondant.
STRING	string
TIMESTAMP	timestamp

Opérateurs

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge les opérateurs suivants.

Opérateurs logiques

- AND
- NOT
- OR

Opérateurs de comparaison

- <

- `>`
- `<=`
- `>=`
- `=`
- `<>`
- `!=`
- `BETWEEN`
- `IN` – Par exemple : `IN ('a', 'b', 'c')`

Opérateurs de correspondance de modèles

- `LIKE`
- `_` (met en correspondance n'importe quel caractère)
- `%` (met en correspondance n'importe quelle séquence de caractères)

Opérateurs unaires

- `IS NULL`
- `IS NOT NULL`

Opérateurs mathématiques

L'addition, la soustraction, la multiplication, la division et les opérateurs modulo sont pris en charge, comme suit :

- `+`
- `-`
- `*`
- `/`
- `%`

Priorité des opérateurs

Le tableau suivant indique la priorité des opérateurs par ordre décroissant.

Opérateur ou élément	Associativité	Obligatoire
`-`	droite	moins unaire
`*`, `/`, `%`	gauche	multiplication, division, opérateur modulo
`+`, `-`	gauche	addition, soustraction
`IN`		appartenance à un ensemble
`BETWEEN`		limitation à une plage
`LIKE`		mise en correspon dance de modèle de chaîne
`<>`		inférieur à, supérieur à
`=`	droite	égalité, affectation
`NOT`	droite	négation logique

Opérateur ou élément	Associativité	Obligatoire
AND	gauche	conjonction logique
OR	gauche	disjonction logique

Mots-clés réservés

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Voici la liste des mots-clés réservés pour Amazon S3 Select. Ces mot-clés comprennent des noms de fonctions, des types de données, des opérateurs, etc. nécessaires pour exécuter les expressions SQL utilisées pour interroger le contenu d'un objet.

```
absolute
action
add
all
allocate
alter
and
any
are
as
asc
assertion
at
authorization
avg
bag
begin
between
```

```
bit
bit_length
blob
bool
boolean
both
by
cascade
cascaded
case
cast
catalog
char
char_length
character
character_length
check
clob
close
coalesce
collate
collation
column
commit
connect
connection
constraint
constraints
continue
convert
corresponding
count
create
cross
current
current_date
current_time
current_timestamp
current_user
cursor
date
day
deallocate
dec
```

```
decimal
declare
default
deferrable
deferred
delete
desc
describe
descriptor
diagnostics
disconnect
distinct
domain
double
drop
else
end
end-exec
escape
except
exception
exec
execute
exists
external
extract
false
fetch
first
float
for
foreign
found
from
full
get
global
go
goto
grant
group
having
hour
identity
```

```
immediate
in
indicator
initially
inner
input
insensitive
insert
int
integer
intersect
interval
into
is
isolation
join
key
language
last
leading
left
level
like
limit
list
local
lower
match
max
min
minute
missing
module
month
names
national
natural
nchar
next
no
not
null
nullif
numeric
```

```
octet_length
of
on
only
open
option
or
order
outer
output
overlaps
pad
partial
pivot
position
precision
prepare
preserve
primary
prior
privileges
procedure
public
read
real
references
relative
restrict
revoke
right
rollback
rows
schema
scroll
second
section
select
session
session_user
set
sexp
size
smallint
some
```

```
space
sql
sqlcode
sqlerror
sqlstate
string
struct
substring
sum
symbol
system_user
table
temporary
then
time
timestamp
timezone_hour
timezone_minute
to
trailing
transaction
translate
translation
trim
true
tuple
union
unique
unknown
unpivot
update
upper
usage
user
using
value
values
varchar
varying
view
when
whenever
where
with
```

```
work
write
year
zone
```

Fonctions SQL

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge les fonctions SQL suivantes.

Rubriques

- Fonctions d'agrégation
- Fonctions conditionnelles
- Fonctions de conversion
- Fonctions de date
- Fonctions de chaîne

Fonctions d'agrégation

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge les fonctions d'agrégation suivantes.

Fonction	Type d'argument	Type de retour
AVG(*expression*)	INT, FLOAT, DECIMAL	DECIMAL pour un argument INT, FLOAT pour un argument de virgule flottante ; sinon, la même chose que le type de données d'argument.
COUNT	-	INT
MAX(*expression*)	INT, DECIMAL	Identique au type d'arguments.
MIN(*expression*)	INT, DECIMAL	Identique au type d'arguments.
SUM(*expression*)	INT, FLOAT, DOUBLE, DECIMAL	INT pour un argument INT, FLOAT pour un argument de virgule flottante ; sinon, la même chose que le type de données d'argument.

Exemple de SUM

Pour agréger la taille totale des objets d'un dossier dans un rapport S3 Inventory, utilisez une expression SUM.

Le rapport S3 Inventory suivant est un fichier CSV compressé avec GZIP. Il comprend trois colonnes.

- La première colonne est le nom du compartiment S3 (*DOC-EXAMPLE-BUCKET*) auquel le rapport S3 Inventory est destiné.
- La deuxième colonne est le nom de clé d'objet qui identifie de façon unique l'objet dans le compartiment.

  La valeur *example-folder/* de la première ligne correspond au dossier *example-folder*. Dans Amazon S3, lorsque vous créez un dossier dans votre compartiment, S3 crée un objet de 0 octet dont la clé est définie par le nom de dossier que vous avez fourni.

  La valeur *example-folder/object1* de la deuxième ligne correspond à l'objet *object1* du dossier *example-folder*.

  La valeur *example-folder/object2* de la troisième ligne correspond à l'objet *object2* du dossier *example-folder*.

  Pour plus d'informations sur les dossiers S3, consultez Organisation des objets dans la console Amazon S3 à l'aide de dossiers.
- La troisième colonne renvoie la taille des objets en octets.

```
"DOC-EXAMPLE-BUCKET","example-folder/","0"
"DOC-EXAMPLE-BUCKET","example-folder/object1","2011267"
"DOC-EXAMPLE-BUCKET","example-folder/object2","1570024"
```

Pour utiliser une expression SUM afin de calculer la taille totale du dossier *example-folder*, exécutez la requête SQL avec Amazon S3 Select.

```
SELECT SUM(CAST(_3 as INT)) FROM s3object s WHERE _2 LIKE 'example-folder/%' AND _2 !=
 'example-folder/';
```

Résultat de la requête :

```
3581291
```

Fonctions conditionnelles

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge les fonctions conditionnelles suivantes.

Rubriques

- CASE
- COALESCE
- NULLIF

CASE

L'expression `CASE` est une expression conditionnelle similaire aux instructions `if/then/else` trouvées dans d'autres langues. `CASE` est utilisé pour spécifier un résultat lorsqu'il y a plusieurs conditions. Il existe deux types d'expressions `CASE` : simple et recherchée.

Dans les expressions `CASE` simples, une expression est comparée à une valeur. Lorsqu'une correspondance est trouvée, l'action spécifiée dans la clause `THEN` est appliquée. Si aucune correspondance n'est trouvée, l'action de la clause `ELSE` est appliquée.

Dans les expressions `CASE` recherchées, chaque `CASE` est évaluée en fonction d'une expression booléenne et l'instruction `CASE` renvoie la première expression `CASE` correspondante. Si aucune correspondance `CASE` n'est trouvée parmi les clauses `WHEN`, l'action contenue dans la clause `ELSE` est renvoyée.

Syntaxe

> **Note**
>
> Actuellement, Amazon S3 Select ne prend pas en charge `ORDER BY` ou les requêtes contenant de nouvelles lignes. Veillez à utiliser des requêtes sans saut de ligne.

Voici une instruction CASE simple qui est utilisée pour faire correspondre les conditions :

```
CASE expression WHEN value THEN result [WHEN...] [ELSE result] END
```

Voici une instruction CASE recherchée utilisée pour évaluer chaque condition :

```
CASE WHEN boolean condition THEN result [WHEN ...] [ELSE result] END
```

Exemples

> **Note**
>
> Si vous utilisez la console Amazon S3 pour exécuter les exemples suivants et que votre fichier CSV contient une ligne d'en-tête, sélectionnez Exclure la première ligne de données CSV.

Exemple 1 : utilisez une simple expression CASE pour remplacer `New York City` par `Big Apple` dans une requête. Remplacer tous les autres noms de villes par `other`.

```
SELECT venuecity, CASE venuecity WHEN 'New York City' THEN 'Big Apple' ELSE 'other' END
 FROM S3Object;
```

Résultat de la requête :

```
venuecity        |   case
-----------------+-----------
Los Angeles      | other
New York City    | Big Apple
San Francisco    | other
Baltimore        | other
...
```

Exemple 2 : utilisez une expression CASE recherchée pour affecter des numéros de groupes basés sur la valeur `pricepaid` pour les ventes de billets individuels :

```
SELECT pricepaid, CASE WHEN CAST(pricepaid as FLOAT) < 10000 THEN 'group 1' WHEN
 CAST(pricepaid as FLOAT) > 10000 THEN 'group 2' ELSE 'group 3' END FROM S3Object;
```

Résultat de la requête :

```
pricepaid |  case
-----------+---------
12624.00 | group 2
10000.00 | group 3
10000.00 | group 3
9996.00 | group 1
9988.00 | group 1
...
```

COALESCE

COALESCE évalue les arguments dans l'ordre et renvoie la première valeur non inconnue, c'est-à-dire la première valeur non nulle ou non manquante. Cette fonction ne propage pas les valeurs nulles ou manquantes.

Syntaxe

```
COALESCE ( expression, expression, ... )
```

Paramètres

expression

Expression cible sur laquelle la fonction opère.

Exemples

```
COALESCE(1)                -- 1
COALESCE(null)             -- null
COALESCE(null, null)       -- null
COALESCE(missing)          -- null
COALESCE(missing, missing) -- null
COALESCE(1, null)          -- 1
COALESCE(null, null, 1)    -- 1
COALESCE(null, 'string')   -- 'string'
COALESCE(missing, 1)       -- 1
```

NULLIF

Pour deux expressions données, NULLIF renvoie NULL si les deux expressions ont la même valeur. Sinon, NULLIF renvoie le résultat de l'évaluation de la première expression.

Syntaxe

```
NULLIF ( expression1, expression2 )
```

Paramètres

expression1, *expression2*

Expressions cible sur lesquelles la fonction opère.

Exemples

```
NULLIF(1, 1)             -- null
NULLIF(1, 2)             -- 1
NULLIF(1.0, 1)           -- null
NULLIF(1, '1')           -- 1
NULLIF([1], [1])         -- null
NULLIF(1, NULL)          -- 1
NULLIF(NULL, 1)          -- null
NULLIF(null, null)       -- null
NULLIF(missing, null)    -- null
NULLIF(missing, missing) -- null
```

Fonctions de conversion

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge la fonction conversationnelle suivante.

Rubriques

- CAST

CAST

La fonction `CAST` convertit une entité, comme une expression analysée comme valeur unique, d'un type à un autre.

Syntaxe

```
CAST ( expression AS data_type )
```

Paramètres

`expression`

Combinaison d'un(e) ou de plusieurs valeurs, opérateurs ou fonctions SQL qui correspondent à une valeur.

`data_type`

Type de données cible, comme `INT`, dans lequel imbriquer l'expression. Pour afficher la liste des types de données pris en charge, consultez Types de données.

Exemples

```
CAST('2007-04-05T14:30Z' AS TIMESTAMP)
CAST(0.456 AS FLOAT)
```

Fonctions de date

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge les fonctions de date suivantes.

Rubriques

- DATE_ADD
- DATE_DIFF

- EXTRACT
- TO_STRING
- TO_TIMESTAMP
- UTCNOW

DATE_ADD

À partir d'une partie de date, d'une quantité et d'un horodatage donnés, `DATE_ADD` renvoie un horodatage mis à jour en remplaçant la partie de date par la quantité.

Syntaxe

```
DATE_ADD( date_part, quantity, timestamp )
```

Paramètres

`date_part`

Spécifie quelle partie de la date modifier. Il peut s'agir de l'une des parties suivantes :

- year
- month
- day
- hour
- minute
- second

`quantity`

Valeur à appliquer à l'horodatage mis à jour. Les valeurs positives de *`quantity`* s'ajoutent à l'élément date_part de l'horodatage et les valeurs négatives se soustraient.

`timestamp`

Horodatage cible sur lequel la fonction opère.

Exemples

```
DATE_ADD(year, 5, `2010-01-01T`)                -- 2015-01-01 (equivalent to
 2015-01-01T)
```

```
DATE_ADD(month, 1, `2010T`)                     -- 2010-02T (result will add precision
 as necessary)
DATE_ADD(month, 13, `2010T`)                    -- 2011-02T
DATE_ADD(day, -1, `2017-01-10T`)                -- 2017-01-09 (equivalent to
 2017-01-09T)
DATE_ADD(hour, 1, `2017T`)                      -- 2017-01-01T01:00-00:00
DATE_ADD(hour, 1, `2017-01-02T03:04Z`)          -- 2017-01-02T04:04Z
DATE_ADD(minute, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:05:05.006Z
DATE_ADD(second, 1, `2017-01-02T03:04:05.006Z`) -- 2017-01-02T03:04:06.006Z
```

DATE_DIFF

À partir d'une partie de date et de deux horodatages valides donnés, `DATE_DIFF` renvoie la différence entre les parties de date. La valeur renvoyée est un entier négatif lorsque la valeur *`date_part`* de *`timestamp1`* est supérieure à la valeur *`date_part`* de *`timestamp2`*. La valeur renvoyée est un entier positif lorsque la valeur *`date_part`* de *`timestamp1`* est inférieure à la valeur *`date_part`* de *`timestamp2`*.

Syntaxe

```
DATE_DIFF( date_part, timestamp1, timestamp2 )
```

Paramètres

`date_part`

Spécifie la partie des horodatages à comparer. Pour obtenir la définition de `date_part`, consultez DATE_ADD.

`timestamp1`

Premier horodatage à comparer.

`timestamp2`

Deuxième horodatage à comparer.

Exemples

```
DATE_DIFF(year, `2010-01-01T`, `2011-01-01T`)           -- 1
DATE_DIFF(year, `2010T`, `2010-05T`)                    -- 4 (2010T is equivalent to
 2010-01-01T00:00:00.000Z)
```

```
DATE_DIFF(month, `2010T`, `2011T`)                      -- 12
DATE_DIFF(month, `2011T`, `2010T`)                      -- -12
DATE_DIFF(day, `2010-01-01T23:00`, `2010-01-02T01:00`) -- 0 (need to be at least 24h
 apart to be 1 day apart)
```

EXTRACT

À partir d'une partie de date et d'un horodatage donnés, EXTRACT renvoie la valeur de la partie de date de l'horodatage.

Syntaxe

```
EXTRACT( date_part FROM timestamp )
```

Paramètres

date_part

Spécifie la partie des horodatages à extraire. Il peut s'agir de l'une des parties suivantes :

- YEAR
- MONTH
- DAY
- HOUR
- MINUTE
- SECOND
- TIMEZONE_HOUR
- TIMEZONE_MINUTE

timestamp

Horodatage cible sur lequel la fonction opère.

Exemples

```
EXTRACT(YEAR FROM `2010-01-01T`)                        -- 2010
EXTRACT(MONTH FROM `2010T`)                             -- 1 (equivalent to
 2010-01-01T00:00:00.000Z)
EXTRACT(MONTH FROM `2010-10T`)                          -- 10
EXTRACT(HOUR FROM `2017-01-02T03:04:05+07:08`)          -- 3
```

```
EXTRACT(MINUTE FROM `2017-01-02T03:04:05+07:08`)           -- 4
EXTRACT(TIMEZONE_HOUR FROM `2017-01-02T03:04:05+07:08`)    -- 7
EXTRACT(TIMEZONE_MINUTE FROM `2017-01-02T03:04:05+07:08`)  -- 8
```

TO_STRING

À partir d'un horodatage et d'un modèle de format donnés, `TO_STRING` renvoie une représentation sous forme de chaîne de l'horodatage au format donné.

Syntaxe

```
TO_STRING ( timestamp time_format_pattern )
```

Paramètres

`timestamp`

Horodatage cible sur lequel la fonction opère.

`time_format_pattern`

Chaîne qui possède les interprétations de caractères spéciaux suivantes :

Format	Exemple	Description
`yy`	`69`	Année sur deux chiffres
`y`	`1969`	Année sur quatre chiffres
`yyyy`	`1969`	Année sur 4 chiffres avec ajout de zéro
`M`	`1`	Mois de l'année
`MM`	`01`	Mois de l'année avec ajout de zéro

Format	Exemple	Description
MMM	Jan	Nom du mois sous forme abrégée
MMMM	January	Nom du mois en entier
MMMMM	J	Première lettre du mois (REMARQUE : ce format n'est pas valide avec la fonction TO_TIMESTAMP .)
d	2	Jour du mois (1-31)
dd	02	Jour du mois avec ajout de zéro (01-31)
a	AM	AM ou PM
h	3	Heure (1-12)
hh	03	Heure avec ajout de zéro (01-12)
H	3	Heure (0-23)
HH	03	Heure avec ajout de zéro (00-23)

Format	Exemple	Description
`m`	`4`	Minutes (0-59)
`mm`	`04`	Minute avec ajout de zéro (00-59)
`s`	`5`	Secondes (0-59)
`ss`	`05`	Seconde avec ajout de zéro (00-59)
`S`	`0`	Fraction de seconde (précision : 0,1, plage : 0,0-0,9)
`SS`	`6`	Fraction de seconde (précision : 0,01, plage : 0,0-0,99)
`SSS`	`60`	Fraction de seconde (précision : 0,001, plage : 0,0-0,999)
…	…	…

Format	Exemple	Description
SSSSSSSSS	60000000	Fraction de seconde (précision maximale : 1 nanoseconde, plage : 0,0-0,999 999999)
n	60000000	Nanoseconde
X	+07 ou Z	Décalage en heures ou Z si le décalage est de 0
XX ou XXXX	+0700 ou Z	Décalage en heures et minutes ou Z si le décalage est de 0
XXX ou XXXXX	+07:00 ou Z	Décalage en heures et minutes ou Z si le décalage est de 0
x	7	Décalage en heures
xx ou xxxx	700	Décalage en heures et minutes

Format	Exemple	Description
xxx ou xxxxx	+07:00	Décalage en heures et minutes

Exemples

```
TO_STRING(`1969-07-20T20:18Z`,  'MMMM d, y')                    -- "July 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMM d, yyyy')                   -- "Jul 20, 1969"
TO_STRING(`1969-07-20T20:18Z`, 'M-d-yy')                        -- "7-20-69"
TO_STRING(`1969-07-20T20:18Z`, 'MM-d-y')                        -- "07-20-1969"
TO_STRING(`1969-07-20T20:18Z`, 'MMMM d, y h:m a')               -- "July 20, 1969 8:18
 PM"
TO_STRING(`1969-07-20T20:18Z`, 'y-MM-dd''T''H:m:ssX')           --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00Z`, 'y-MM-dd''T''H:m:ssX')     --
 "1969-07-20T20:18:00Z"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXX')   --
 "1969-07-20T20:18:00+0800"
TO_STRING(`1969-07-20T20:18+08:00`, 'y-MM-dd''T''H:m:ssXXXXX')  --
 "1969-07-20T20:18:00+08:00"
```

TO_TIMESTAMP

À partir d'une chaîne donnée, `TO_TIMESTAMP` le convertit en un horodatage. `TO_TIMESTAMP` est l'opération inverse de `TO_STRING`.

Syntaxe

```
TO_TIMESTAMP ( string )
```

Paramètres

`string`

Chaîne cible sur laquelle la fonction opère.

Exemples

```
TO_TIMESTAMP('2007T')                          -- `2007T`
TO_TIMESTAMP('2007-02-23T12:14:33.079-08:00') -- `2007-02-23T12:14:33.079-08:00`
```

UTCNOW

`UTCNOW` renvoie l'heure actuelle au format UTC sous forme d'horodatage.

Syntaxe

```
UTCNOW()
```

Paramètres

`UTCNOW` n'accepte aucun paramètre.

Exemples

```
UTCNOW() -- 2017-10-13T16:02:11.123Z
```

Fonctions de chaîne

> **Important**
>
> Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus

Amazon S3 Select prend en charge les fonctions de chaîne suivantes.

Rubriques

- CHAR_LENGTH, CHARACTER_LENGTH
- LOWER
- SUBSTRING
- TRIM

- UPPER

CHAR_LENGTH, CHARACTER_LENGTH

CHAR_LENGTH (ou CHARACTER_LENGTH) compte le nombre de caractères dans la chaîne spécifiée.

> **Note**
>
> CHAR_LENGTH et CHARACTER_LENGTH sont synonymes.

Syntaxe

```
CHAR_LENGTH ( string )
```

Paramètres

string

Chaîne cible sur laquelle la fonction opère.

Exemples

```
CHAR_LENGTH('')          -- 0
CHAR_LENGTH('abcdefg')   -- 7
```

LOWER

À partir d'une chaîne donnée, LOWER convertit tous les caractères majuscules en minuscules. Les caractères qui ne sont pas en majuscules restent inchangés.

Syntaxe

```
LOWER ( string )
```

Paramètres

string

Chaîne cible sur laquelle la fonction opère.

Exemples

```
LOWER('AbCdEfG!@#$') -- 'abcdefg!@#$'
```

SUBSTRING

À partir d'une chaîne, d'un index de début et éventuellement d'une longueur donnés, `SUBSTRING` renvoie la sous-chaîne de l'index de début à la fin de la chaîne ou à la fin de la longueur précisée.

> **Note**
>
> Le premier caractère de la chaîne d'entrée possède la position d'index 1.
>
> - Si `start` est < 1, sans longueur spécifiée, la position d'index est définie sur 1.
> - Si `start` est < 1, avec une longueur spécifiée, la position d'index est définie sur `start + length -1`.
> - Si `start + length -1` est < 0, une chaîne vide est renvoyée.
> - Si `start + length -1` est > = 0, la sous-chaîne commençant à la position d'index 1 dont la longueur est `start + length - 1` est renvoyée.

Syntaxe

```
SUBSTRING( string FROM start [ FOR length ] )
```

Paramètres

`string`

Chaîne cible sur laquelle la fonction opère.

`start`

Position de début de la chaîne.

`length`

Longueur de la sous-chaîne à renvoyer. En cas d'absence du paramètre, le traitement s'effectue jusqu'à la fin de la chaîne.

Exemples

```
SUBSTRING("123456789", 0)      -- "123456789"
SUBSTRING("123456789", 1)      -- "123456789"
SUBSTRING("123456789", 2)      -- "23456789"
SUBSTRING("123456789", -4)     -- "123456789"
SUBSTRING("123456789", 0, 999) -- "123456789"
SUBSTRING("123456789", 1, 5)   -- "12345"
```

TRIM

Supprime les caractères de tête ou de fin d'une chaîne. Le caractère par défaut à supprimer est un espace (`' '`).

Syntaxe

```
TRIM ( [[LEADING | TRAILING | BOTH remove_chars] FROM] string )
```

Paramètres

`string`

Chaîne cible sur laquelle la fonction opère.

`LEADING | TRAILING | BOTH`

Ce paramètre indique s'il faut supprimer les caractères de tête ou de fin ou les deux.

`remove_chars`

Jeu de caractères à supprimer. *`remove_chars`* peut être une chaîne de longueur > 1. Cette fonction renvoie la chaîne avec n'importe quel caractère de *`remove_chars`* se trouvant au début ou à la fin de la chaîne qui a été supprimée.

Exemples

```
TRIM('       foobar         ')              -- 'foobar'
TRIM('      \tfoobar\t         ')           -- '\tfoobar\t'
TRIM(LEADING FROM '       foobar         ')  -- 'foobar         '
TRIM(TRAILING FROM '       foobar         ') -- '       foobar'
TRIM(BOTH FROM '       foobar         ')     -- 'foobar'
TRIM(BOTH '12' FROM '1112211foobar22211122') -- 'foobar'
```

UPPER

À partir d'une chaîne donnée, UPPER convertit tous les caractères minuscules en majuscules. Les caractères qui ne sont pas en minuscules restent inchangés.

Syntaxe

```
UPPER ( string )
```

Paramètres

string

Chaîne cible sur laquelle la fonction opère.

Exemples

```
UPPER('AbCdEfG!@#$') -- 'ABCDEFG!@#$'
```

Utilisation des compartiments de répertoires

Les compartiments de répertoires organisent les données de manière hiérarchique dans des répertoires, contrairement à la structure de stockage horizontale des compartiments à usage général. Il n'existe pas de limite de préfixe pour les compartiments de répertoires et les répertoires individuels peuvent faire l'objet d'une mise à l'échelle horizontale.

Vous pouvez créer jusqu'à 100 compartiments de répertoire dans chacun de vos répertoires Comptes AWS, sans limite quant au nombre d'objets que vous pouvez stocker dans un compartiment. Votre quota de compartiments est appliqué à chaque région dans votre Compte AWS. Si votre application nécessite une augmentation de cette limite, contactez Support.

> **Important**
>
> Les compartiments d'annuaire situés dans des zones de disponibilité qui n'ont aucune activité de demande pendant une période d'au moins 90 jours passent à l'état inactif. Lorsqu'il est dans un état inactif, un compartiment de répertoires est temporairement inaccessible pour les lectures et les écritures. Les compartiments inactifs conservent tout le stockage, ainsi que toutes les métadonnées d'objet et de compartiment. Les frais de stockage existants s'appliqueront aux compartiments inactifs. Si vous envoyez une demande d'accès à un compartiment inactif, ce dernier passera à l'état actif, généralement en quelques minutes. Pendant cette période de transition, les lectures et les écritures renverront un code d'erreur `503 (Service Unavailable)`. Cela ne s'applique pas aux compartiments situés dans les Zones Locales.

Il existe plusieurs types de compartiments Amazon S3. Avant de créer un bucket, assurez-vous de choisir le type de bucket qui correspond le mieux à votre application et à vos exigences de performance. Pour plus d'informations sur les différents types de bucket et les cas d'utilisation appropriés pour chacun, consultezCompartiments.

Les rubriques suivantes fournissent des informations sur les compartiments de répertoires. Pour plus d'informations sur les compartiments à usage général, consultez Présentation des compartiments à usage général.

Pour plus d'informations sur les compartiments de répertoires, consultez les rubriques suivantes.

- Noms des compartiments de répertoires

- Annuaires
- Noms de clés
- Gestion des accès

Noms des compartiments de répertoires

Le nom d'un compartiment de répertoires se compose d'un nom de base que vous fournissez et d'un suffixe contenant l'ID de la zone (zone de disponibilité ou zone locale) dans laquelle se trouve votre compartiment. Les noms de compartiments de répertoires doivent utiliser le format suivant et respecter les règles de dénomination des compartiments de répertoires :

```
bucket-base-name--zone-id--x-s3
```

Par exemple, le nom de compartiment de répertoires suivant contient l'ID de zone de disponibilité `usw2-az1` :

```
bucket-base-name--usw2-az1--x-s3
```

Pour de plus amples informations, veuillez consulter Règles de dénomination des compartiments de répertoires.

Annuaires

Les compartiments de répertoires organisent les données de manière hiérarchique dans des répertoires, contrairement à la structure de tri horizontale des compartiments à usage général.

Avec un espace de noms hiérarchique, le délimiteur figurant dans la clé d'objet est important. Le seul délimiteur pris en charge est la barre oblique (`/`). Les répertoires sont déterminés par les limites des délimiteurs. Par exemple, la clé d'objet `dir1/dir2/file1.txt` entraîne la création automatique des répertoires `dir1/` et `dir2/`, et l'ajout de l'objet `file1.txt` dans le répertoire `/dir2`, dans le chemin `dir1/dir2/file1.txt`.

Le modèle d'indexation des compartiments de répertoires renvoie des résultats non triés pour l'opération d'API `ListObjectsV2`. Si vous devez limiter vos résultats à une sous-section de votre compartiment, vous pouvez spécifier un chemin de sous-répertoire dans le paramètre `prefix`, par exemple, `prefix=dir1/`.

Noms de clés

Pour les compartiments de répertoires, les sous-répertoires communs à plusieurs clés d'objet sont créés avec la première clé d'objet. Les clés d'objet supplémentaires pour le même sous-répertoire utilisent le sous-répertoire créé précédemment. Ce modèle vous permet de choisir les clés d'objet les mieux adaptées à l'application, avec une prise en charge égale des répertoires fragmentés et denses.

Gestion des accès

Les compartiments de répertoires ont tous les paramètres de blocage de l'accès public S3 activés par défaut au niveau des compartiments. La propriété de l'objet S3 est définie pour être appliquée par le propriétaire du compartiment et les listes de contrôle d'accès (ACLs) sont désactivées. Ces paramètres ne peuvent pas être modifiés.

Par défaut, les utilisateurs ne disposent pas d'autorisations pour les compartiments de répertoires. Pour accorder des autorisations d'accès pour les compartiments de répertoires, vous pouvez utiliser IAM pour créer des utilisateurs, des groupes ou des rôles, et attacher des autorisations à ces identités. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM.

Vous pouvez également contrôler l'accès aux compartiments de répertoire par le biais de points d'accès. Les points d'accès simplifient la gestion de l'accès aux données à grande échelle pour les ensembles de données partagés dans Amazon S3. Les points d'accès sont des noms d'hôtes uniques que vous créez pour appliquer des autorisations et des contrôles réseau distincts pour toutes les demandes effectuées via un point d'accès. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux ensembles de données partagés dans des compartiments d'annuaire dotés de points d'accès.

Quotas de compartiments de répertoires

Les quotas, également appelés limites, sont le nombre maximum de ressources de service ou d'opérations pour vous Compte AWS. Les quotas pour les compartiments de répertoire sont les suivants. Pour plus d'informations sur les quotas dans Amazon S3, consultez la section Quotas Amazon S3.

Nom	Par défaut	Ajustable	Description
Compartiments de répertoires	Chaque compte : 100	Oui	Le nombre de compartiments d'annuaire Amazon S3 que vous pouvez créer dans un compte.
Lire le TPS par compartiment de répertoire	Chaque compartiment de répertoire : jusqu'à 200 000 TPS de lecture	Pour demander une augmentation de quota, contactez le Support.	Le nombre de GET/HEAD demandes par seconde par compartiment de répertoire.
Écrire le TPS par compartiment de répertoire	Chaque compartiment de répertoire : jusqu'à 100 000 TPS en écriture	Pour demander une augmentation de quota, contactez le Support.	Le nombre de PUT/DELETE demandes par seconde par compartiment de répertoire.

Création et utilisation de compartiments de répertoires

Pour plus d'informations sur l'utilisation des compartiments de répertoires, consultez les rubriques suivantes.

- Cas d'utilisation des compartiments de répertoires
- Différences pour les compartiments de répertoires
- Mise en réseau des compartiments de répertoires
- Règles de dénomination des compartiments de répertoires
- Affichage des propriétés d'un compartiment de répertoires
- Gestion des politiques des compartiments de répertoires
- Vidage d'un compartiment de répertoires
- Suppression d'un compartiment de répertoires
- Établissement de la liste des compartiments de répertoires

- Déterminer si vous pouvez accéder à un compartiment de répertoires
- Utilisation d'objets dans un compartiment de répertoires
- Sécurité des compartiments de répertoires
- Gestion de l'accès aux ensembles de données partagés dans des compartiments d'annuaire dotés de points d'accès
- Optimisation des performances des compartiments de répertoires
- Développement avec des compartiments de répertoires
- Utilisation de balises avec des compartiments de répertoire S3

Cas d'utilisation des compartiments de répertoires

Les compartiments de répertoires prennent en charge la création de compartiments dans les types d'emplacement de compartiment suivants : zone de disponibilité ou zone locale.

Pour les cas d'utilisation à faible latence, vous pouvez créer un compartiment de répertoires dans une seule zone de disponibilité pour stocker les données. Les compartiments de répertoires figurant dans des zones de disponibilité prennent en charge la classe de stockage S3 Express One Zone. La classe de stockage S3 Express One Zone est recommandée si votre application est sensible aux performances et peut bénéficier d'une latence inférieure à dix millisecondes pour les demandes `PUT` et `GET`. Pour en savoir plus sur la création de compartiments de répertoires dans les zones de disponibilité, consultez Charges de travail hautes performances.

Pour les cas d'utilisation liés à la résidence des données, vous pouvez créer un bucket de répertoire dans une seule zone locale AWS dédiée (DLZ) pour stocker les données. Les compartiments de répertoires des zones locales prennent en charge la classe de stockage S3 One Zone-Infrequent Access (S3 One Zone-IA ; Z-IA). Pour en savoir plus sur la création de compartiments de répertoires dans les zones locales, consultez Charges de travail liées à la résidence des données.

Rubriques

- Charges de travail hautes performances
- Charges de travail liées à la résidence des données

Charges de travail hautes performances

S3 Express One Zone

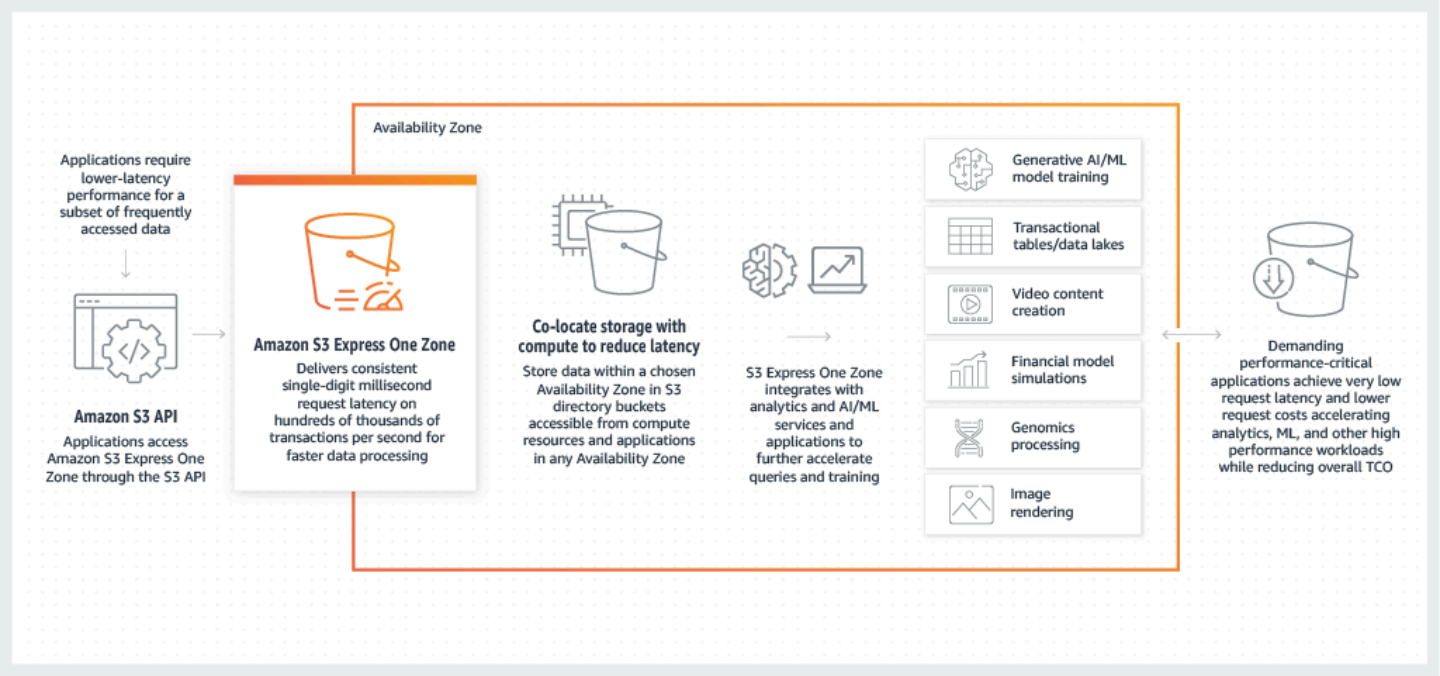
Vous pouvez utiliser Amazon S3 Express One Zone pour les charges de travail hautes performances. S3 Express One Zone est la première classe de stockage S3 dans laquelle vous pouvez sélectionner une zone de disponibilité unique avec la possibilité de regrouper le stockage d'objets et les ressources de calcul, ce qui assure la vitesse d'accès la plus élevée possible. Les objets figurant dans S3 Express One Zone sont stockés dans des compartiments de répertoires situés dans des zones de disponibilité. Pour plus d'informations sur les compartiments de répertoires, consultez Compartiments de répertoires.

Amazon S3 Express One Zone est une classe de stockage Amazon S3 à zone unique et hautes performances, spécialement conçue pour fournir un accès aux données constant en moins de dix millisecondes pour vos applications les plus sensibles à la latence. S3 Express One Zone est la classe de stockage d'objets cloud qui présente la latence la plus faible à l'heure actuelle, avec une vitesse d'accès aux données jusqu'à 10 fois plus grande et des coûts de demande 50 % inférieurs à ceux de S3 Standard. Les applications peuvent bénéficier immédiatement d'une accélération des demandes. S3 Express One Zone offre une élasticité des performances similaire à celle des autres classes de stockage S3. S3 Express One Zone est utilisé pour les charges de travail ou les applications critiques en termes de performances qui nécessitent une latence constante inférieure à dix millisecondes.

Comme avec les classes de stockage Amazon S3, vous n'avez pas besoin de planifier ni de provisionner à l'avance les exigences en matière de capacité ou de débit. Vous pouvez augmenter ou diminuer la capacité de stockage en fonction de vos besoins, et accéder à vos données via les API Amazon S3.

La classe de stockage Amazon S3 Express One Zone est conçue pour garantir une disponibilité de 99,95 % au sein d'une même zone de disponibilité et s'appuie sur le contrat de niveau de service Amazon S3. Avec S3 Express One Zone, vos données sont stockées de façon redondante sur plusieurs appareils au sein d'une même zone de disponibilité. S3 Express One Zone est conçu pour gérer les défaillances simultanées de périphériques en détectant et réparant rapidement toute perte de redondance. En cas de panne de l'appareil existant, S3 Express One Zone transfère automatiquement les demandes vers de nouveaux appareils au sein d'une zone de disponibilité. Cette redondance permet de garantir un accès ininterrompu à vos données au sein d'une zone de disponibilité.

S3 Express One Zone est idéal pour toute application où il est important de réduire au maximum la latence requise pour accéder à un objet. Il peut s'agir de flux de travail impliquant des interactions avec des utilisateurs, tels que le montage vidéo, où les créatifs ont besoin d'un accès réactif au contenu à partir de leur interface utilisateur. S3 Express One Zone profite également aux charges de travail d'analytique et de machine learning qui ont des exigences similaires en matière de réactivité de leurs données, notamment aux charges de travail présentant de nombreux petits accès ou un grand nombre d'accès aléatoires. S3 Express One Zone peut être utilisé avec d'autres Services AWS pour prendre en charge les charges de travail d'analyse, d'intelligence artificielle et d'apprentissage automatique (AI/ML), telles qu'Amazon EMR, Amazon AI SageMaker et Amazon Athena.



Pour les compartiments de répertoires qui utilisent la classe de stockage S3 Express One Zone, les données sont stockées sur plusieurs appareils au sein d'une même zone de disponibilité, mais elles ne sont pas stockées de manière redondante entre les zones de disponibilité. Lorsque vous créez un bucket d'annuaire pour utiliser la classe de stockage S3 Express One Zone, nous vous recommandons de spécifier une Région AWS et une zone de disponibilité locales pour vos instances de calcul Amazon EC2, Amazon Elastic Kubernetes Service ou Amazon Elastic Container Service (Amazon ECS) afin d'optimiser les performances.

Lorsque vous utilisez S3 Express One Zone, vous pouvez interagir avec votre compartiment de répertoires dans un cloud privé virtuel (VPC) à l'aide d'un point de terminaison de VPC de passerelle. Avec un point de terminaison de passerelle, vous pouvez accéder à des compartiments de répertoires S3 Express One Zone à partir de votre VPC sans passerelle Internet ni périphérique NAT pour votre VPC, sans frais supplémentaires.

Avec les compartiments de répertoires, vous pouvez utiliser un grand nombre des fonctionnalités et API Amazon S3 que vous utilisez avec les compartiments à usage général et les autres classes de stockage. Il s'agit notamment de Mountpoint pour Amazon S3, du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), du chiffrement côté serveur avec des clés () AWS Key Management Service (SSE-KMS), des AWS KMS opérations par lots S3 et de S3 Block Public Access. Vous pouvez accéder à S3 Express One Zone à l'aide de la console Amazon S3 AWS Command Line Interface (AWS CLI) et de l'API REST Amazon S3. AWS SDKs

Pour plus d'informations sur S3 Express One Zone, consultez les rubriques suivantes.

- Présentation
- Fonctionnalités de S3 Express One Zone
- Services connexes
- Étapes suivantes

Présentation

Pour optimiser les performances et réduire la latence, S3 Express One Zone introduit les nouveaux concepts suivants.

Zones de disponibilité

La classe de stockage Amazon S3 Express One Zone est conçue pour garantir une disponibilité de 99,95 % au sein d'une même zone de disponibilité et s'appuie sur le contrat de niveau de service Amazon S3. Avec S3 Express One Zone, vos données sont stockées de façon redondante sur plusieurs appareils au sein d'une même zone de disponibilité. S3 Express One Zone est conçu pour gérer les défaillances simultanées de périphériques en détectant et réparant rapidement toute perte de redondance. En cas de panne de l'appareil existant, S3 Express One Zone transfère automatiquement les demandes vers de nouveaux appareils au sein d'une zone de disponibilité. Cette redondance permet de garantir un accès ininterrompu à vos données au sein d'une zone de disponibilité.

Une zone de disponibilité est un ou plusieurs centres de données discrets dotés d'une alimentation, d'un réseau et d'une connectivité redondants dans une Région AWS. Lorsque vous créez un bucket d'annuaire, vous choisissez la zone de disponibilité et Région AWS l'emplacement de votre bucket.

Zone de disponibilité unique

Lorsque vous créez un compartiment de répertoires, vous choisissez la zone de disponibilité et la Région AWS.

Les compartiments de répertoires utilisent la classe de stockage S3 Express One Zone, conçue pour être utilisée par des applications sensibles aux performances. S3 Express One Zone est la première classe de stockage S3 dans laquelle vous pouvez sélectionner une zone de disponibilité unique avec la possibilité de regrouper le stockage d'objets et les ressources de calcul, ce qui assure la vitesse d'accès la plus élevée possible.

Avec S3 Express One Zone, vos données sont stockées de façon redondante sur plusieurs appareils au sein d'une même zone de disponibilité. S3 Express One Zone est conçu pour garantir une disponibilité de 99,95 % au sein d'une même zone de disponibilité et s'appuie sur le contrat de niveau de service Amazon S3. Pour de plus amples informations, consultez Zones de disponibilité.

Points de terminaison et points de terminaison de VPC de passerelle

Les opérations d'API de gestion des compartiments de répertoires sont disponibles via un point de terminaison régional et sont appelées API de point de terminaison régional. `CreateBucket` et `DeleteBucket` sont des exemples d'opérations d'API de point de terminaison régional. Après avoir créé un compartiment de répertoires, vous pouvez utiliser les opérations d'API de point de terminaison zonal pour charger et gérer les objets dans votre compartiment de répertoires. Les opérations d'API de point de terminaison zonal sont disponibles via un point de terminaison zonal. `PutObject` et `CopyObject` sont des exemples d'opérations d'API de point de terminaison zonal.

Vous pouvez accéder à S3 Express One Zone à partir de votre VPC en utilisant des points de terminaison de VPC de passerelle. Après avoir créé un point de terminaison de passerelle, vous pouvez l'ajouter comme cible dans votre table de routage pour le trafic destiné à S3 Express One Zone depuis votre VPC. Comme avec Amazon S3, aucuns frais supplémentaires ne s'appliquent à l'utilisation de points de terminaison de passerelle. Pour plus d'informations sur la manière de configurer des points de terminaison de VPC de passerelle, consultez Mise en réseau des compartiments de répertoires.

Autorisation basée sur les sessions

Avec S3 Express One Zone, vous authentifiez et autorisez les demandes par le biais d'un nouveau mécanisme basé sur les sessions, optimisé pour assurer une latence minimale. Vous pouvez utiliser `CreateSession` pour demander des informations d'identification temporaires afin de bénéficier

d'un accès à faible latence à votre compartiment. Ces informations d'identification temporaires sont limitées à un compartiment de répertoires S3 spécifique. Les jetons de session sont utilisés uniquement avec les opérations zonales (niveau objet) (à l'exception de CopyObject). Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison zonal avec `CreateSession`.

Le service pris en AWS SDKs charge par S3 Express One Zone gère l'établissement et le rafraîchissement des sessions en votre nom. Pour protéger vos sessions, les informations d'identification de sécurité temporaires expirent au bout de 5 minutes. Après avoir téléchargé, installé AWS SDKs et configuré les autorisations AWS Identity and Access Management (IAM) nécessaires, vous pouvez immédiatement commencer à utiliser les opérations d'API.

Fonctionnalités de S3 Express One Zone

Les fonctionnalités S3 suivantes sont disponibles pour S3 Express One Zone. Pour obtenir la liste complète des opérations d'API prises en charge et des fonctionnalités non prises en charge, consultez Différences pour les compartiments de répertoires.

Gestion des accès et sécurité

Vous pouvez utiliser les fonctionnalités suivantes pour auditer et gérer l'accès. Par défaut, les compartiments de répertoires sont privés et sont accessibles uniquement par les utilisateurs auxquels l'accès a été explicitement accordé. Contrairement aux compartiments à usage général, qui peuvent définir la limite de contrôle d'accès au niveau des compartiments, des préfixes ou des balises d'objet, la limite de contrôle d'accès pour les compartiments de répertoires est définie uniquement au niveau des compartiments. Pour plus d'informations, consultez Autorisation des opérations d'API de point de terminaison régional avec IAM.

- Blocage de l'accès public S3 : tous les paramètres de blocage de l'accès public S3 sont activés par défaut au niveau des compartiments. Ce paramètre par défaut ne peut pas être modifié.
- Propriété des objets S3 (propriétaire du compartiment appliqué par défaut) : les listes de contrôle d'accès (ACLs) ne sont pas prises en charge pour les compartiments d'annuaire. Les compartiments de répertoires utilisent automatiquement le paramètre Propriétaire du compartiment appliqué pour la propriété des objets S3. L'application par le propriétaire du compartiment signifie qu' ACLs elle est désactivée, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. Ce paramètre par défaut ne peut pas être modifié.
- AWS Identity and Access Management (IAM) — IAM vous aide à contrôler en toute sécurité l'accès à vos compartiments d'annuaire. Vous pouvez utiliser IAM pour accorder l'accès aux

opérations d'API (régionales) de gestion des compartiments et aux opérations d'API (zonales) de gestion des objets via l'action `s3express:CreateSession`. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM. Contrairement aux actions de gestion d'objets, les actions de gestion de compartiments ne peuvent pas être effectuées entre comptes. Seul le propriétaire du compartiment peut effectuer ces actions.

- Politiques de compartiment : utilisez un langage de politique basé sur IAM afin de configurer les autorisations basées sur les ressources pour vos compartiments de répertoires. Vous pouvez également utiliser IAM pour contrôler l'accès à l'opération d'API `CreateSession` qui vous permet d'utiliser les opérations d'API de gestion des objets ou de gestion par zone. Vous pouvez accorder un accès intercompte ou un accès dans le même compte aux opérations d'API zonales. Pour plus d'informations sur les politiques et les autorisations S3 Express One Zone, consultez Autorisation des opérations d'API de point de terminaison régional avec IAM.
- Analyseur d'accès IAM pour S3 : évaluez et surveillez vos stratégies d'accès pour vous assurer qu'elles fournissent uniquement l'accès prévu à vos ressources S3.

Journalisation et surveillance

S3 Express One Zone utilise les outils de journalisation et de surveillance S3 suivant pour surveiller et contrôler la façon dont vos ressources sont utilisées :

- Amazon CloudWatch Metrics — Surveillez vos AWS ressources et vos applications en les utilisant CloudWatch pour collecter et suivre les métriques. S3 Express One Zone utilise le même espace de CloudWatch noms que les autres classes de stockage Amazon S3 (`AWS/S3`) et prend en charge les métriques de stockage quotidiennes pour les compartiments de répertoire : `BucketSizeBytes` et. `NumberOfObjects` Pour de plus amples informations, veuillez consulter Surveillance des métriques avec Amazon CloudWatch.
- AWS CloudTrail logs — AWS CloudTrail est un outil Service AWS qui vous aide à mettre en œuvre l'audit opérationnel et des risques, la gouvernance et la conformité de votre entreprise Compte AWS en enregistrant les actions entreprises par un utilisateur, un rôle ou un Service AWS. Pour S3 Express One Zone, CloudTrail capture les opérations d'API de point de terminaison régional (par exemple, `CreateBucket` et`PutBucketPolicy`) en tant qu'événements de gestion et les opérations d'API zonales (par exemple, `GetObject` et`PutObject`) en tant qu'événements de données. Ces événements incluent les actions entreprises dans le cadre des opérations AWS Management Console AWS SDKs, AWS Command Line Interface (AWS CLI) et de AWS l'API. Pour plus d'informations, consultez Logging with AWS CloudTrail for S3 Express One Zone.

> **Note**
>
> Les journaux d'accès au serveur Amazon S3 ne sont pas pris en charge avec S3 Express One Zone.

Gestion des objets

Vous pouvez gérer votre stockage d'objets à l'aide de la console Amazon S3 AWS SDKs, et AWS CLI. Les fonctionnalités suivantes sont disponibles pour la gestion des objets avec S3 Express One Zone :

- Opérations par lots S3 : utilisez les opérations par lots pour effectuer des opérations groupées sur des objets dans des compartiments de répertoire, par exemple, la AWS Lambda fonction Copy and Invoke. Par exemple, vous pouvez utiliser les opérations par lots pour copier des objets entre des compartiments de répertoires et des compartiments à usage général. Avec Batch Operations, vous pouvez gérer des milliards d'objets à grande échelle avec une seule requête S3 en utilisant AWS SDKs AWS CLI ou en quelques clics dans la console Amazon S3.
- Importation : après avoir créé un compartiment de répertoires, vous pouvez le remplir d'objets à l'aide de la fonctionnalité d'importation dans la console Amazon S3. L'importation est une méthode simplifiée pour créer des tâches d'opérations par lots afin de copier des objets depuis des compartiments à usage général vers des compartiments de répertoires.

AWS SDKs et bibliothèques clientes

Vous pouvez gérer votre stockage d'objets à l'aide des bibliothèques clientes AWS SDKs et.

- Mountpoint pour Amazon S3 : Mountpoint pour Amazon S3 est un client de fichiers open source qui fournit un accès à haut débit, réduisant ainsi les coûts de calcul pour les lacs de données sur Amazon S3. Mountpoint pour Amazon S3 traduit les appels d'API du système de fichiers local en appels d'API d'objet S3 tels que `GET` et `LIST`. Il est idéal pour les charges de travail de lacs de données à lecture intense qui traitent des pétaoctets de données et qui nécessitent le débit élastique élevé fourni par Amazon S3 pour pouvoir augmenter et réduire la capacité de milliers d'instances.
- S3A : S3A est une interface compatible Hadoop recommandée pour accéder aux magasins de données dans Amazon S3. S3A remplace le client du système de fichiers S3N Hadoop.

- PyTorchon AWS — PyTorch on AWS est un framework d'apprentissage profond open source qui facilite le développement de modèles d'apprentissage automatique et leur déploiement en production.
- AWS SDKs— Vous pouvez l'utiliser AWS SDKs lorsque vous développez des applications avec Amazon S3. AWS SDKsSimplifiez vos tâches de programmation en encapsulant l'API REST Amazon S3 sous-jacente. Pour plus d'informations sur l'utilisation de la zone AWS SDKs avec S3 Express One, consultezthe section called "AWS SDKs".

Chiffrement et protection des données

Les objets dans S3 Express One Zone sont automatiquement chiffrés par chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). S3 Express One Zone prend également en charge le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). S3 Express One Zone ne prend pas en charge le chiffrement côté serveur avec des clés de chiffrement (SSE-C) fournies par le client, ni le chiffrement double couche côté serveur avec AWS KMS keys (DSSE-KMS). Pour de plus amples informations, veuillez consulter Protection et chiffrement des données.

S3 Express One Zone vous offre la possibilité de choisir l'algorithme de somme de contrôle utilisé pour valider vos données pendant le chargement ou le téléchargement. Vous pouvez sélectionner l'un des algorithmes de hachage sécurisé (SHA) ou de contrôle de redondance cyclique (CRC) suivants : CRC32 C CRC32, SHA-1 et SHA-256. MD5les checksums basés sur la classe de stockage S3 Express One Zone ne sont pas pris en charge.

Pour de plus amples informations, veuillez consulter Bonnes pratiques supplémentaires en matière de somme de contrôle S3.

AWS Version de signature (4SigV4)

S3 Express One Zone utilise AWS la version de signature 4 (SigV4). SigV4est un protocole de signature utilisé pour authentifier les demandes adressées à Amazon S3 via HTTPS. S3 Express One Zone signe les demandes en utilisant AWS Sigv4. Pour plus d'informations, consultez Authentification des demandes (AWS Signature version 4) dans le manuel Amazon Simple Storage Service API Reference.

Forte cohérence

S3 Express One Zone assure une forte read-after-write cohérence pour l'ensemble des objets contenus dans vos compartiments de répertoire PUT et pour les DELETE Régions AWS requêtes y

afférentes. Pour de plus amples informations, veuillez consulter Modèle de cohérence des données Amazon S3.

Services connexes

Vous pouvez utiliser ce qui suit Services AWS avec la classe de stockage S3 Express One Zone pour prendre en charge votre cas d'utilisation spécifique à faible latence.

- Amazon Elastic Compute Cloud (Amazon EC2) — Amazon EC2 fournit une capacité de calcul sécurisée et évolutive dans le AWS Cloud. L'utilisation d'Amazon EC2 réduit le besoin d'investir dans du matériel dès le départ, ce qui vous permet de développer et de déployer des applications plus rapidement. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que nécessaire, configurer la sécurité et le réseau, et gérer le stockage.
- AWS Lambda : Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs. 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.
- Amazon Elastic Kubernetes Service (Amazon EKS) — Amazon EKS est un service géré qui élimine le besoin d'installer, d'exploiter et de maintenir Kubernetes votre propre plan de contrôle. AWSKubernetesest un système open source qui automatise la gestion, le dimensionnement et le déploiement des applications conteneurisées.
- Amazon Elastic Container Service (Amazon ECS) : Amazon ECS est un service d'orchestration de conteneurs entièrement géré qui vous permet de déployer, de gérer et de mettre à l'échelle aisément des applications conteneurisées.
- AWS Service de gestion des clés (AWS KMS) — Le service de gestion des AWS clés (AWS KMS) est un service AWS géré qui vous permet de créer et de contrôler facilement les clés de chiffrement utilisées pour chiffrer vos données. Les clés AWS KMS que vous créez dans AWS KMS sont protégées par des modules matériels de sécurité (HSM) validés par la norme FIPS 140-2. Pour utiliser ou gérer vos clés KMS, vous devez interagir avec AWS KMS.
- Amazon Athena : Amazon Athena est un service de requête interactif qui facilite l'analyse des données directement dans Amazon S3 à l'aide du langage SQL standard. Vous pouvez également utiliser Athena pour exécuter de façon interactive l'analytique des données à l'aide d'Apache Spark sans avoir à planifier, configurer ni gérer de ressources. Lorsque vous exécutez des applications Apache Spark sur Athena, vous soumettez du code Spark pour traitement et recevez directement les résultats.

- Amazon SageMaker Training : passez en revue les options relatives aux modèles de formation avec AmazonSageMaker, notamment les algorithmes intégrés, les algorithmes personnalisés, les bibliothèques et les modèles issus du AWS Marketplace.
- AWS Glue— AWS Glue est un service d'intégration de données sans serveur qui permet aux utilisateurs d'outils d'analyse de découvrir, de préparer, de déplacer et d'intégrer facilement des données provenant de sources multiples. Vous pouvez l'utiliser AWS Glue pour l'analyse, l'apprentissage automatique et le développement d'applications. AWS Glue inclut également des outils de productivité et d'exploitation des données supplémentaires pour la création, l'exécution de tâches et la mise en œuvre de flux de travail commerciaux.
- Amazon EMR — Amazon EMR est une plate-forme de clusters gérés qui simplifie l'exécution de frameworks de mégadonnées, tels que le traitement Apache Hadoop et Apache Spark l'analyse AWS de grandes quantités de données.
- AWS CloudTrail— AWS CloudTrail est un AWS service qui vous aide à permettre l'audit opérationnel et des risques, la gouvernance et la conformité de votre AWS compte. Les actions entreprises par un utilisateur, un rôle ou un AWS service sont enregistrées sous forme d'événements dans CloudTrail. Les événements incluent les actions entreprises dans la console AWS de gestion, l'interface de ligne de AWS commande AWS SDKs et APIs.
- AWS CloudFormation — est un service qui vous aide à modéliser et à configurer vos AWS ressources afin que vous puissiez passer moins de temps à les gérer et plus de temps à vous concentrer sur les applications qui s'exécutent AWS. Vous créez un modèle qui décrit toutes les AWS ressources que vous souhaitez (comme les EC2 instances Amazon ou les instances de base de données Amazon RDS), et vous vous CloudFormation occupez du provisionnement et de la configuration de ces ressources pour vous. Vous n'avez pas besoin de créer et de configurer AWS des ressources individuellement et de déterminer ce qui dépend de quoi ; il CloudFormation gère tout cela.

Étapes suivantes

Pour plus d'informations sur l'utilisation des compartiments de répertoires et de la classe de stockage S3 Express One Zone, consultez les rubriques suivantes :

- Didacticiel : bien démarrer avec S3 Express One Zone
- Régions et zones de disponibilité S3 Express One Zone
- Mise en réseau des compartiments de répertoires dans une zone de disponibilité
- Création de compartiments de répertoires dans une zone de disponibilité

- Points de terminaison régionaux et zonaux pour les compartiments de répertoires d'une zone de disponibilité
- Optimisation des performances de S3 Express One Zone

Didacticiel : bien démarrer avec S3 Express One Zone

Amazon S3 Express One Zone est la première classe de stockage S3 dans laquelle vous pouvez sélectionner une zone de disponibilité unique avec la possibilité de regrouper le stockage d'objets et les ressources de calcul, ce qui assure la vitesse d'accès la plus élevée possible. Les données figurant dans S3 Express One Zone sont stockées dans des compartiments de répertoires situés dans des zones de disponibilité. Pour plus d'informations sur les compartiments de répertoires, consultez Compartiments de répertoires.

S3 Express One Zone est idéal pour toute application où il est crucial de réduire au maximum la latence des demandes. Il peut s'agir de flux de travail impliquant des interactions avec des utilisateurs, tels que le montage vidéo, où les créatifs ont besoin d'un accès réactif au contenu à partir de leur interface utilisateur. S3 Express One Zone profite également aux charges de travail d'analytique et de machine learning qui ont des exigences similaires en matière de réactivité de leurs données, notamment aux charges de travail présentant de nombreux petits accès ou un grand nombre d'accès aléatoires. S3 Express One Zone peut être utilisé avec d'autres AWS services tels qu'Amazon EMR, Amazon Athena AWS , Glue Data Catalog et SageMaker Amazon Model Training pour prendre en charge les charges de travail d'analyse, d'intelligence artificielle et d'apprentissage automatique (AI/ML). Vous pouvez utiliser la classe de stockage et les compartiments de répertoire S3 Express One Zone à l'aide de la console Amazon S3 AWS SDKs, de l'interface de ligne de AWS commande (AWS CLI) et de l'API REST Amazon S3. Pour plus d'informations, consultez les sections Qu'est-ce que S3 Express One Zone ? et En quoi S3 Express One Zone est-il différent ?.
Voici le schéma d'un flux de travail S3 Express One Zone.

Objectif

Dans ce didacticiel, vous apprendrez à créer un point de terminaison de passerelle, à créer et à joindre une politique IAM, à créer un compartiment de répertoires, puis à utiliser l'action d'importation pour remplir votre compartiment de répertoire avec des objets stockés dans un compartiment à usage général. Vous pouvez également charger des objets manuellement dans votre compartiment de répertoires.

Rubriques

- Prérequis

- Étape 1 : configurer un point de terminaison VPC de passerelle pour accéder aux compartiments de répertoire S3 Express One Zone
- Étape 2 : Création d'un bucket de répertoire S3 Express One Zone
- Étape 3 : Importation de données dans un bucket d'annuaire S3 Express One Zone
- Étape 4 : Chargez manuellement des objets dans votre compartiment de répertoire S3 Express One Zone
- Étape 5 : Videz votre bucket de répertoire S3 Express One Zone
- Étape 6 : Supprimer votre bucket de répertoire S3 Express One Zone
- Étapes suivantes

Prérequis

Avant de commencer ce didacticiel, vous devez disposer d'un utilisateur Compte AWS auquel vous pouvez vous connecter en tant qu'utilisateur AWS Identity and Access Management (IAM) avec les autorisations appropriées.

Sous-étapes

- Créez un Compte AWS
- Création d'un utilisateur IAM dans votre Compte AWS (console)
- Création d'une politique IAM et association de cette politique à un utilisateur ou rôle IAM (console)

Créez un Compte AWS

Pour terminer ce didacticiel, vous avez besoin d'un Compte AWS. Lorsque vous vous inscrivez AWS, vous êtes automatiquement Compte AWS inscrit à tous les services AWS, y compris Amazon S3. Seuls les services que vous utilisez vous sont facturés. Pour plus d'informations sur la tarification, consultez Tarification S3.

Création d'un utilisateur IAM dans votre Compte AWS (console)

AWS Identity and Access Management (IAM) est un outil Service AWS qui aide les administrateurs à contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (via les autorisations nécessaires) à accéder aux objets et à utiliser les compartiments de répertoires dans S3 Express One Zone. Vous pouvez utiliser IAM sans frais supplémentaires.

Par défaut, les utilisateurs ne disposent pas d'autorisations pour accéder aux compartiments de répertoires ni aux opérations S3 Express One Zone. Pour accorder des autorisations d'accès pour les compartiments de répertoires et les opérations S3 Express One Zone, vous pouvez utiliser IAM pour créer des utilisateurs ou des rôles et associer des autorisations à ces identités. Pour en savoir plus sur la création d'un utilisateur IAM, consultez Créer des utilisateurs IAM (console) dans le guide de l'utilisateur IAM. Pour plus d'informations sur la création d'un rôle IAM, consultez Création d'un rôle pour la délégation d'autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM.

Pour des raisons de simplicité, ce didacticiel crée et utilise un utilisateur IAM. Après avoir terminé ce didacticiel, n'oubliez pas de Supprimer l'utilisateur IAM. Pour une utilisation en production, nous vous recommandons de suivre les Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM. Une bonne pratique requiert que les utilisateurs humains utilisent une fédération avec un fournisseur d'identité pour accéder à AWS avec des informations d'identification temporaires. Une autre bonne pratique consiste à exiger que les charges de travail utilisent des informations d'identification temporaires avec des rôles IAM pour accéder à AWS. Pour en savoir plus sur l'utilisation AWS IAM Identity Center pour créer des utilisateurs dotés d'informations d'identification temporaires, consultez la section Mise en route dans le guide de AWS IAM Identity Center l'utilisateur.

> **Warning**
>
> Les utilisateurs IAM disposent d'informations d'identification à long terme, ce qui présente un risque de sécurité. Pour atténuer ce risque, nous vous recommandons de ne fournir à ces utilisateurs que les autorisations dont ils ont besoin pour effectuer la tâche et de supprimer ces autorisations lorsqu'elles ne sont plus nécessaires.

Création d'une politique IAM et association de cette politique à un utilisateur ou rôle IAM (console)

Par défaut, les utilisateurs ne disposent pas d'autorisations pour les compartiments de répertoires et les opérations S3 Express One Zone. Pour accorder des autorisations d'accès pour les compartiments de répertoires, vous pouvez utiliser IAM pour créer des utilisateurs, des groupes ou des rôles, et attacher des autorisations à ces identités. Les compartiments de répertoires sont la seule ressource que vous pouvez inclure dans les politiques de compartiment ou les politiques d'identité IAM pour accéder à S3 Express One Zone.

Pour utiliser les opérations d'API de point de terminaison régional (opérations au niveau des compartiments ou du plan de contrôle) avec S3 Express One Zone, vous utilisez le modèle

d'autorisation IAM, qui n'implique aucune gestion des sessions. Les autorisations sont accordées pour les actions, de façon individuelle. Pour utiliser les opérations d'API de point de terminaison zonal (opérations au niveau des objets ou du plan de données), vous utilisez l'opération d'API `CreateSession` pour créer et gérer des sessions optimisées afin d'autoriser les demandes de données à faible latence. Pour récupérer et utiliser un jeton de session, vous devez autoriser l'action `s3express:CreateSession` pour votre compartiment de répertoires dans une politique basée sur l'identité ou une politique de compartiment. Si vous accédez à S3 Express One Zone depuis la console Amazon S3, via l'interface de ligne de AWS commande (AWS CLI) ou en utilisant la AWS SDKs, S3 Express One Zone crée une session en votre nom. Pour plus d'informations, consultez Autorisation `CreateSession` et Gestion des identités et des accès AWS (AWS IAM) pour S3 Express One Zone.

Pour créer une politique IAM et l'associer à un utilisateur ou rôle IAM (console)

1. Connectez-vous à la console AWS de gestion et ouvrez la console de gestion IAM.
2. Dans le volet de navigation, choisissez Politiques.
3. Choisissez Create Policy (Créer une politique).
4. Sélectionnez JSON.
5. Copiez la politique ci-dessous dans la fenêtre de l'éditeur de politique. Avant de créer des compartiments de répertoire ou d'utiliser S3 Express One Zone, vous devez accorder les autorisations nécessaires à votre rôle AWS Identity and Access Management (IAM) ou à vos utilisateurs. Cet exemple de politique autorise l'accès à l'opération d'API `CreateSession` (à utiliser avec d'autres opérations d'API de point de terminaison zonal ou au niveau des objets) et à toutes les opérations d'API de point de terminaison régional (au niveau des compartiments). Cette politique autorise l'utilisation de l'opération d'API `CreateSession` avec tous les compartiments de répertoires, mais les opérations d'API de point de terminaison régional sont autorisées à être utilisées uniquement avec le compartiment de répertoires spécifié. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

   JSON

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

```
            "Effect": "Allow",
            "Action": [
                "s3express:DeleteBucket",
                "s3express:DeleteBucketPolicy",
                "s3express:CreateBucket",
                "s3express:PutBucketPolicy",
                "s3express:GetBucketPolicy",
                "s3express:ListAllMyDirectoryBuckets"
            ],

            "Resource": "arn:aws:s3express:aws-
region:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3/*"
        },
        {
            "Sid": "AllowCreateSession",
            "Effect": "Allow",
            "Action": "s3express:CreateSession",
            "Resource": "*"
        }
    ]
}
```

6. Choisissez Suivant.
7. Nommez la politique.

> **Note**
>
> Les balises de compartiment ne sont pas prises en charge pour S3 Express One Zone.

8. Sélectionnez Create Policy (Créer une politique).
9. Maintenant que vous avez créé une politique IAM, vous pouvez l'attacher à un utilisateur IAM. Dans le volet de navigation, choisissez Politiques.
10. Dans la barre de recherche, saisissez le nom de la politique.
11. Dans le menu Actions, sélectionnez Attacher.
12. Sous Filtrer par type d'entité, sélectionnez Utilisateurs IAM ou Rôles.
13. Dans le champ de recherche, saisissez le nom de l'utilisateur ou du rôle que vous souhaitez utiliser.
14. Choisissez Attach Policy (Attacher une politique).

Étape 1 : configurer un point de terminaison VPC de passerelle pour accéder aux compartiments de répertoire S3 Express One Zone

Vous pouvez accéder aux opérations d'API zonales et régionales via des points de terminaison de cloud privé virtuel (VPC) de passerelle. Les points de terminaison de passerelle permettent au trafic d'atteindre S3 Express One Zone sans passer par une passerelle NAT. Nous vous recommandons vivement d'utiliser des points de terminaison de passerelle, car ils fournissent le chemin réseau le plus optimal lorsque vous travaillez avec S3 Express One Zone. Vous pouvez accéder à des compartiments de répertoires S3 Express One Zone à partir de votre VPC sans passerelle Internet ni périphérique NAT pour votre VPC, sans frais supplémentaires. Utilisez la procédure suivante pour configurer un point de terminaison de passerelle qui se connecte à des compartiments de répertoires et des objets de la classe de stockage S3 Express One Zone.

Pour accéder à S3 Express One Zone, vous utilisez des points de terminaison régionaux et zonaux différents des points de terminaison Amazon S3 standard. Selon l'opération d'API Amazon S3 que vous utilisez, un point de terminaison zonal ou régional est requis. Pour obtenir la liste complète des opérations d'API prises en charge par type de point de terminaison, consultez Opérations d'API prises en charge par S3 Express One Zone. Vous devez accéder aux points de terminaison zonaux et régionaux via un point de terminaison de cloud privé virtuel (VPC) de passerelle.

Utilisez la procédure suivante pour créer un point de terminaison de passerelle qui se connecte à des compartiments de répertoires et des objets de la classe de stockage S3 Express One Zone.

Pour configurer un point de terminaison de VPC de passerelle

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation latéral, sous Cloud privé virtuel, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Créez un nom pour votre point de terminaison.
5. Pour Service category (Catégorie de service), choisissez Services AWS.
6. Sous Services, effectuez une recherche à l'aide du filtre Type=Gateway, puis choisissez le bouton d'option à côté de com.amazonaws. ***region***.s3 express.
7. Pour VPC, choisissez le VPC dans lequel créer le point de terminaison.
8. Pour Configure route tables (Configurer les tables de routage), sélectionnez les tables de routage qui seront utilisées par le point de terminaison. Amazon VPC ajoute automatiquement une route pour pointer le trafic destiné au service vers l'interface réseau du point de terminaison.

9. Pour Politique, choisissez Accès complet afin d'autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, choisissez Personnalisé pour attacher une politique de point de terminaison de VPC qui contrôle les autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le point de terminaison de VPC.
10. Choisissez Créer un point de terminaison.

Après avoir créé un point de terminaison de passerelle, vous pouvez utiliser les points de terminaison d'API régionaux et les points de terminaison d'API zonaux pour accéder aux compartiments de répertoires et aux objets de classe de stockage Amazon S3 Express One Zone.

Étape 2 : Création d'un bucket de répertoire S3 Express One Zone

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.

   > **Note**
   >
   > Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste d'Amazon S3 Régions AWS, consultez la section sur les Service AWS points de terminaison dans le Référence générale d'Amazon Web Services.

3. Dans le volet de navigation de gauche, choisissez Directory buckets.
4. Choisissez Créer un compartiment. La page Créer un compartiment s'ouvre.
5. Sous Configuration générale, consultez l' Région AWS endroit où votre bucket sera créé.

   Sous Type de compartiment, choisissez Répertoire.

   > **Note**
   >
   > - Si vous avez choisi une région qui ne prend pas en charge les compartiments de répertoires, l'option Type de compartiment disparaît, et le type de compartiment est défini par défaut sur un compartiment à usage général. Pour créer un compartiment

de répertoires, vous devez choisir une région prise en charge. Pour obtenir la liste des régions qui prennent en charge les compartiments de répertoires et la classe de stockage Amazon S3 Express One Zone, consultez the section called "Régions et zones de disponibilité S3 Express One Zone".

- Une fois que vous avez créé le compartiment, vous ne pouvez pas modifier son type.

> **Note**
>
> La zone de disponibilité ne peut pas être modifiée une fois le compartiment créé.

6. Pour Zone de disponibilité, choisissez une zone de disponibilité locale pour vos services de calcul. Pour obtenir la liste des zones de disponibilité qui prennent en charge les compartiments de répertoires et la classe de stockage S3 Express One Zone, consultez the section called "Régions et zones de disponibilité S3 Express One Zone".

   Sous Zone de disponibilité, cochez la case confirmant que vous comprenez qu'en cas de panne de la zone de disponibilité, vos données pourraient être indisponibles ou perdues.

   > **Important**
   >
   > Les compartiments de répertoires sont stockés sur plusieurs appareils au sein d'une même zone de disponibilité, mais ne stockent pas les données de manière redondante entre les zones de disponibilité.

7. Pour Nom du compartiment, entrez un nom pour votre compartiment de répertoires.

   Les règles suivantes s'appliquent pour nommer les compartiments de répertoires :

   - Soyez unique au sein de la zone choisie (zone de AWS disponibilité ou zone AWS locale).
   - Le nom doit contenir entre 3 (minimum) et 63 caractères (maximum), suffixe inclus.
   - Doit être composé uniquement de lettres minuscules, de chiffres et de traits d'union (-).
   - Il doit commencer et se terminer par une lettre ou un chiffre.
   - Doit inclure le suffixe suivant : `--`*`zone-id`*`--x-s3`
   - Les noms de compartiment ne doivent pas commencer par le préfixe `xn--`.
   - Les noms de compartiment ne doivent pas commencer par le préfixe `sthree-`.

- Les noms de compartiment ne doivent pas commencer par le préfixe `sthree-configurator`.
- Les noms de compartiment ne doivent pas commencer par le préfixe `amzn-s3-demo-`.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `-s3alias`. Ce suffixe est réservé aux noms d'alias de point d'accès. Pour plus d'informations, consultez Alias de point d'accès.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `--ol-s3`. Ce suffixe est réservé aux noms d'alias de point d'accès Object Lambda. Pour de plus amples informations, veuillez consulter Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda de compartiment S3.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `.mrap`. Ce suffixe est réservé aux noms de point d'accès multi-régions. Pour de plus amples informations, veuillez consulter Règles relatives à l'attribution de noms pour les points d'accès multi-Régions Amazon S3.

Un suffixe est automatiquement ajouté au nom de base que vous fournissez lorsque vous créez un compartiment de répertoires à l'aide de la console. Ce suffixe inclut l'ID de la zone de disponibilité que vous avez choisie.

Une fois le compartiment créé, vous ne pouvez pas changer son nom. Pour plus d'informations sur l'attribution de noms à des compartiments, consultez Règles de dénomination des compartiments à usage général.

> **Important**
>
> N'ajoutez pas d'informations sensibles, notamment des numéros de compte, dans le nom du compartiment. Le nom du bucket est visible URLs là où pointent les objets du bucket.

8. Sous Propriété de l'objet, le paramètre imposé au propriétaire du compartiment est automatiquement activé et toutes les listes de contrôle d'accès (ACLs) sont désactivées. Impossible d'activer les ACLs compartiments de répertoire.

   Application par le propriétaire du compartiment (par défaut) : ACLs cette option est désactivée, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment à usage général et en a le contrôle total. ACLs n'affectent plus les autorisations d'accès

aux données du compartiment à usage général S3. Le compartiment utilise des stratégies exclusivement pour définir le contrôle des accès.

9. Sous Paramètres de blocage de l'accès public pour ce compartiment, notez que les paramètres de blocage de l'accès public pour votre compartiment de répertoires sont automatiquement activés. Ces paramètres ne peuvent pas être modifiés pour les compartiments de répertoires. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.
10. Pour configurer le chiffrement par défaut, dans Type de chiffrement, choisissez l'une des options suivantes :

    - Chiffrement côté serveur avec clé gérée Amazon S3 (SSE-S3)
    - Chiffrement côté serveur avec AWS Key Management Service clé (SSE-KMS)

    Pour en savoir plus sur l'utilisation du chiffrement côté serveur Amazon S3 pour chiffrer vos données, consultez Protection et chiffrement des données.

    > **Important**
    >
    > Si vous utilisez l'option SSE-KMS pour votre configuration de chiffrement par défaut, vous êtes soumis aux quotas RPS (demandes par seconde) de AWS KMS. Pour plus d'informations sur les quotas de AWS KMS et sur la procédure à suivre pour demander une augmentation des quotas, consultez Quotas dans le Guide du développeur AWS Key Management Service .
    > Lorsque vous activez le chiffrement par défaut, vous devrez peut-être mettre à jour votre politique de compartiment. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement SSE-KMS pour les opérations intercomptes.

11. Si vous avez choisi le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), sous Bucket Key, Enabled apparaît. Les clés de compartiment S3 sont toujours activées lorsque vous configurez votre compartiment d'annuaire pour utiliser le chiffrement par défaut avec SSE-S3. Les clés de compartiment S3 sont toujours activées pour les opérations `GET` et `PUT` dans un compartiment de répertoires et ne peuvent pas être désactivées. Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de CopyObject, d'UploadPartCopy, de l'opération

Copy dans les opérations par lot ou des tâches import. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS.

Les clés de compartiment S3 réduisent le coût du chiffrement en diminuant le trafic de demandes d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

12. Si vous avez choisi le chiffrement côté serveur avec AWS Key Management Service clé (SSE-KMS), sous AWS KMS clé, spécifiez votre AWS Key Management Service clé de l'une des manières suivantes ou créez-en une nouvelle.

    - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans Disponible AWS KMS keys.

      Seules les clés gérées par vos clients apparaissent dans cette liste. Le Clé gérée par AWS (`aws/s3`) n'est pas pris en charge dans les compartiments de répertoire. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .
    - Pour saisir l'ARN ou l'alias de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN ou l'alias de votre clé KMS dans AWS KMS key ARN.
    - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

      Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

    > ⚠ Important
    >
    > - Votre configuration SSE-KMS ne peut prendre en charge qu'une seule clé gérée par le client par compartiment de répertoires pendant toute la durée de vie du compartiment. La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. De même, après avoir spécifié une clé gérée par le client pour SSE-KMS, vous ne pouvez pas remplacer la clé gérée par le client pour la configuration SSE-KMS du compartiment.
>
>   Vous pouvez identifier la clé gérée par le client que vous avez spécifiée pour la configuration SSE-KMS du compartiment de la manière suivante :
>
>   - Effectuez une demande d'opération d'API `HeadObject` pour trouver la valeur de `x-amz-server-side-encryption-aws-kms-key-id` dans la réponse.

Pour utiliser une nouvelle clé gérée par le client pour vos données, nous vous recommandons de copier vos objets existants dans un nouveau compartiment de répertoires avec une nouvelle clé gérée par le client.

- Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez d'abord avoir l'autorisation d'utiliser cette clé, puis vous devez saisir l'ARN de la clé KMS. Pour plus d'informations sur les autorisations entre comptes pour les clés KMS, consultez Création de clés KMS que d'autres comptes peuvent utiliser dans le Guide du développeur AWS Key Management Service . Pour en savoir plus sur SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) pour les chargements de nouveaux objets dans des compartiments de répertoires.
- Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans des compartiments de répertoire, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez Identification des clés KMS symétriques et asymétriques dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur l'utilisation AWS KMS avec Amazon S3, consultezUtilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de répertoire.

13. Choisissez Créer un compartiment. Après avoir créé le compartiment, vous pouvez y ajouter des fichiers et des dossiers. Pour de plus amples informations, veuillez consulter the section called "Utilisation d'objets dans un compartiment de répertoires".

Étape 3 : Importation de données dans un bucket d'annuaire S3 Express One Zone

Pour effectuer cette étape, vous devez disposer d'un bucket à usage général contenant des objets et situé dans le même emplacement Région AWS que votre bucket de répertoire.

Après avoir créé un compartiment de répertoires dans Amazon S3, vous pouvez remplir le nouveau compartiment avec des données à l'aide de l'action d'importation dans la console Amazon S3.

L'importation simplifie la copie de données dans des compartiments de répertoires en vous permettant de choisir un préfixe ou un compartiment à usage général à partir duquel importer les données sans avoir à spécifier tous les objets à copier individuellement. L'importation utilise les opérations par lot S3, qui copient les objets dans le préfixe ou le compartiment à usage général sélectionné. Vous pouvez suivre la progression de la tâche de la copie d'importation via la page de détails de la tâche d'opérations par lot S3.

Pour utiliser l'action Importer

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, sélectionnez le nom de la Région AWS actuellement affichée. Choisissez ensuite la région associée à la zone de disponibilité dans laquelle se trouve votre compartiment de répertoires.
3. Dans le volet de navigation de gauche, choisissez Directory buckets.
4. Cliquez sur le bouton d'option situé à côté du nom du compartiment dans lequel vous souhaitez importer des objets.
5. Choisissez Importer.
6. Pour Source, entrez le compartiment à usage général (ou le chemin du compartiment, préfixe inclus) qui contient les objets que vous souhaitez importer. Pour choisir un compartiment à usage général existant dans une liste, choisissez Parcourir S3.
7. Dans la section Autorisations, vous pouvez choisir de générer automatiquement un rôle IAM. Vous pouvez également sélectionner un rôle IAM dans une liste ou saisir directement l'ARN d'un rôle IAM.

   - Pour autoriser Amazon S3 à créer un nouveau rôle IAM en votre nom, choisissez Créer un nouveau rôle IAM.

     > **Note**
     >
     > Si vos objets sources sont chiffrés avec un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), ne choisissez pas l'option Créer un nouveau rôle IAM. Spécifiez plutôt un rôle IAM existant disposant de l'autorisation `kms:Decrypt`.

Amazon S3 utilisera cette autorisation pour déchiffrer vos objets. Pendant le processus d'importation, Amazon S3 rechiffrera ensuite ces objets à l'aide d'un chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3).

- Pour choisir un rôle IAM existant dans une liste, choisissez Sélectionner parmi les rôles IAM existants.
- Pour spécifier un rôle IAM existant en entrant son Amazon Resource Name (ARN), choisissez Saisir l'ARN du rôle IAM, puis entrez l'ARN dans le champ correspondant.

8. Passez en revue les informations affichées dans les sections Destination et Paramètres de l'objet copié. Si les informations de la section Destination sont correctes, choisissez Importer pour démarrer la tâche de copie.

   La console Amazon S3 affiche le statut de votre nouvelle tâche sur la page Opérations par lot. Pour plus d'informations sur la tâche, choisissez le bouton d'option à côté du nom de la tâche, puis dans le menu Actions, choisissez Afficher les détails. Pour ouvrir le compartiment de répertoires dans lequel les objets seront importés, choisissez Afficher la destination de l'importation.

Étape 4 : Chargez manuellement des objets dans votre compartiment de répertoire S3 Express One Zone

Vous pouvez aussi charger des objets manuellement dans votre compartiment de répertoires.

Pour charger manuellement des objets

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation située dans le coin supérieur droit de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région associée à la zone de disponibilité dans laquelle se trouve votre compartiment de répertoires.
3. Dans le volet de navigation de gauche, choisissez Directory buckets.
4. Choisissez le nom du compartiment dans lequel vous souhaitez charger vos dossiers ou fichiers.

> **Note**
>
> Si vous avez choisi le même compartiment de répertoires que celui que vous avez utilisé dans les étapes précédentes de ce didacticiel, votre compartiment de répertoires contient

les objets qui ont été chargés à partir de l'outil d'importation. Notez que ces objets sont désormais stockés dans la classe de stockage S3 Express One Zone.

5. Dans l'onglet Objets, choisissez Charger.
6. Sur la page Charger, procédez de l'une des manières suivantes :
   - Faites glisser et déposez les fichiers et les dossiers dans la fenêtre de chargement.
   - Choisissez Ajouter des fichiers ou Ajouter un dossier, puis choisissez les fichiers ou les dossiers à charger et sélectionnez Ouvrir ou Charger.
7. Sous Sommes de contrôle, choisissez la fonction de somme de contrôle que vous souhaitez utiliser.

   > **Note**
   >
   > Nous vous recommandons d'utiliser CRC32 et CRC32 C pour obtenir les meilleures performances avec la classe de stockage S3 Express One Zone. Pour plus d'informations, consultez Bonnes pratiques en matière de sommes de contrôle supplémentaires S3.

   (Facultatif) Si vous importez un seul objet d'une taille inférieure à 16 Mo, vous pouvez également spécifier une valeur de somme de contrôle précalculée. Lorsque vous fournissez une valeur précalculée, Amazon S3 la compare à la valeur calculée à l'aide de la fonction de somme de contrôle sélectionnée. Si les valeurs ne correspondent pas, le chargement ne démarrera pas.
8. Les options des sections Autorisations et Propriétés sont automatiquement définies selon les paramètres par défaut et ne peuvent pas être modifiées. Le blocage de l'accès public est automatiquement activé, et la gestion des versions S3 ainsi que le verrouillage d'objet S3 ne peuvent pas être activés pour les compartiments de répertoires.

   (Facultatif) Si vous souhaitez ajouter des métadonnées sous forme de paires clé-valeur aux objets, développez la section Propriétés, puis dans la section Métadonnées, choisissez Ajouter des métadonnées.
9. Pour charger les fichiers et dossiers répertoriés, choisissez Charger.

   Amazon S3 charge les objets et les dossiers. Lorsque le chargement est terminé, un message de réussite s'affiche sur la page Charger : statut.

Vous avez créé avec succès un compartiment de répertoires et y avez chargé des objets.

Étape 5 : Videz votre bucket de répertoire S3 Express One Zone

Vous pouvez vider un compartiment de répertoires Amazon S3 à l'aide de la console Amazon S3.

Pour vider un compartiment de répertoires.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation située dans le coin supérieur droit de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région associée à la zone de disponibilité dans laquelle se trouve votre compartiment de répertoires.
3. Dans le volet de navigation de gauche, choisissez Directory buckets.
4. Choisissez la case d'option située à côté du nom du compartiment à vider, puis choisissez Vider.
5. Dans la page Empty bucket (Vider le compartiment), confirmez que vous souhaitez vider le compartiment en saisissant **`permanently delete`** dans le champ de texte, puis choisissez Empty (Vider).
6. Surveillez la progression du processus de vidage du compartiment sur la page Vider le compartiment : état.

Étape 6 : Supprimer votre bucket de répertoire S3 Express One Zone

Une fois que vous avez vidé votre compartiment de répertoires et que vous avez abandonné tous les chargements partitionnés en cours, vous pouvez supprimer le compartiment à l'aide de la console Amazon S3.

Pour supprimer un compartiment de répertoires

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation située dans le coin supérieur droit de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région associée à la zone de disponibilité dans laquelle se trouve votre compartiment de répertoires.
3. Dans le volet de navigation de gauche, choisissez Directory buckets.

4. Dans la liste Compartiments de répertoires, choisissez la case d'option située à côté du compartiment que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Sur la page Supprimer le compartiment, saisissez le nom du compartiment dans le champ de texte pour confirmer la suppression de ce compartiment.

   > **Important**
   >
   > La suppression d'un compartiment de répertoires ne peut pas être annulée.

7. Pour supprimer votre compartiment de répertoires, choisissez Supprimer le compartiment.

Étapes suivantes

Dans ce didacticiel, vous avez appris à créer un compartiment de répertoires et à utiliser la classe de stockage S3 Express One Zone. Au terme ce didacticiel, vous pourrez explorer les services AWS connexes à utiliser avec la classe de stockage S3 Express One Zone.

Vous pouvez utiliser ce qui suit Services AWS avec la classe de stockage S3 Express One Zone pour prendre en charge votre cas d'utilisation spécifique à faible latence.

- Amazon Elastic Compute Cloud (Amazon EC2) — Amazon EC2 fournit une capacité de calcul sécurisée et évolutive dans le AWS Cloud. L'utilisation d'Amazon EC2 réduit le besoin d'investir dans du matériel dès le départ, ce qui vous permet de développer et de déployer des applications plus rapidement. Vous pouvez utiliser Amazon EC2 pour lancer autant ou aussi peu de serveurs virtuels que nécessaire, configurer la sécurité et le réseau, et gérer le stockage.
- AWS Lambda : Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs. 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.
- Amazon Elastic Kubernetes Service (Amazon EKS) — Amazon EKS est un service géré qui élimine le besoin d'installer, d'exploiter et de maintenir Kubernetes votre propre plan de contrôle. AWSKubernetesest un système open source qui automatise la gestion, le dimensionnement et le déploiement des applications conteneurisées.
- Amazon Elastic Container Service (Amazon ECS) : Amazon ECS est un service d'orchestration de conteneurs entièrement géré qui vous permet de déployer, de gérer et de mettre à l'échelle aisément des applications conteneurisées.

- Amazon EMR — Amazon EMR est une plate-forme de clusters gérés qui simplifie l'exécution de frameworks de mégadonnées, tels que Apache Spark le traitement Apache Hadoop et l'analyse AWS de grandes quantités de données.
- Amazon Athena : Amazon Athena est un service de requête interactif qui facilite l'analyse des données directement dans Amazon S3 à l'aide du langage SQL standard. Vous pouvez également utiliser Athena pour exécuter de façon interactive l'analytique des données à l'aide d'Apache Spark sans avoir à planifier, configurer ni gérer de ressources. Lorsque vous exécutez des applications Apache Spark sur Athena, vous soumettez du code Spark pour traitement et recevez directement les résultats.
- AWS Glue Data Catalog AWS Glue est un service d'intégration de données sans serveur qui permet aux utilisateurs d'outils d'analyse de découvrir, de préparer, de déplacer et d'intégrer facilement des données provenant de sources multiples. Vous pouvez l'utiliser AWS Glue pour l'analyse, l'apprentissage automatique et le développement d'applications. AWS Glue Data Catalog est un référentiel centralisé qui stocke les métadonnées relatives aux ensembles de données de votre organisation. Il sert d'index pour l'emplacement, le schéma et les métriques d'exécution de vos sources de données.
- Amazon SageMaker Runtime Model Training — Amazon SageMaker Runtime est un service d'apprentissage automatique entièrement géré. Avec SageMaker Runtime, les data scientists et les développeurs peuvent rapidement et facilement créer et entraîner des modèles d'apprentissage automatique, puis les déployer directement dans un environnement hébergé prêt pour la production.

Pour plus d'informations sur S3 Express One Zone, consultez les sections Qu'est-ce que S3 Express One Zone ? et En quoi S3 Express One Zone est-il différent ?.

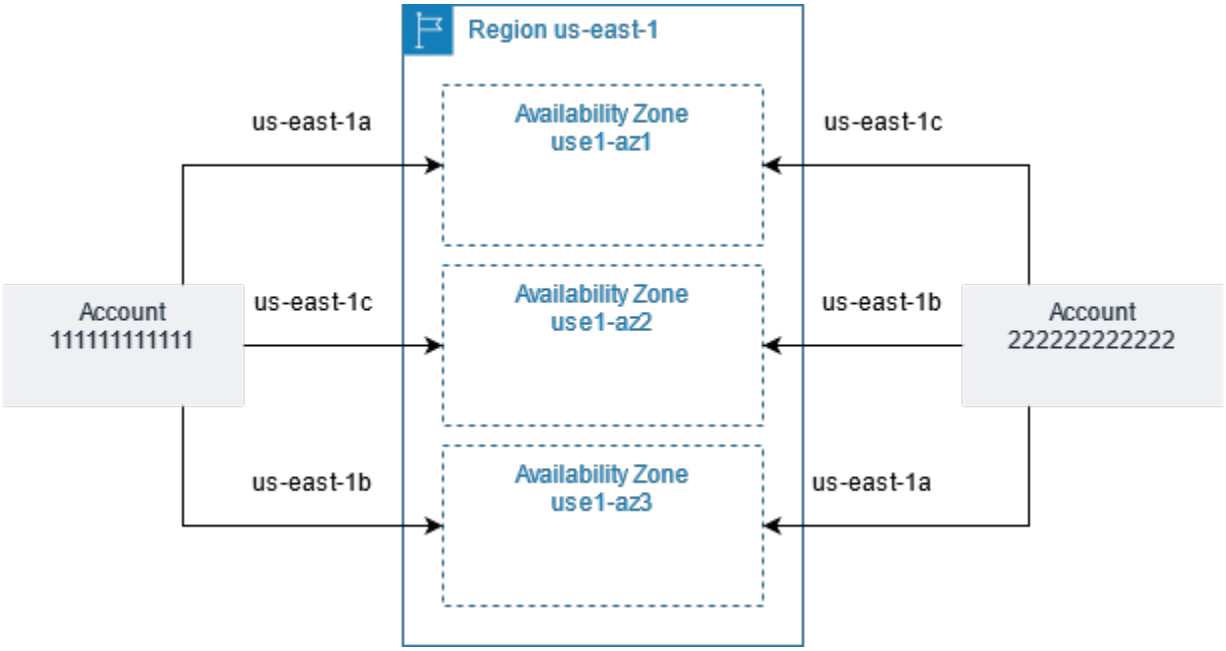
Régions et zones de disponibilité S3 Express One Zone

Une zone de disponibilité est un ou plusieurs centres de données discrets dotés d'une alimentation, d'un réseau et d'une connectivité redondants dans une Région AWS. Pour optimiser les récupérations à faible latence, les objets de la classe de stockage Amazon S3 Express One Zone sont stockés de manière redondante dans des compartiments de répertoires S3 dans une zone de disponibilité unique locale à votre charge de travail de calcul. Lorsque vous créez un bucket d'annuaire, vous choisissez la zone de disponibilité et Région AWS l'emplacement de votre bucket.

AWS fait correspondre les zones de disponibilité physiques de manière aléatoire aux noms des zones de disponibilité de chacune d'entre elles Compte AWS. Cette approche permet de répartir les ressources entre les zones de disponibilité au lieu de concentrer les ressources dans la première

zone de disponibilité de chaque région. Région AWS Par conséquent, il est Compte AWS possible que la zone `us-east-1a` de disponibilité de votre site ne représente pas le même emplacement physique que celle `us-east-1a` d'une autre Compte AWS. Pour plus d'informations, consultez la section Régions et zones de disponibilité dans le guide de EC2 l'utilisateur Amazon.

Pour coordonner les zones de disponibilité entre les comptes, vous devez utiliser un ID de zone de disponibilité, qui représente l'identifiant unique et cohérent d'une zone de disponibilité. Par exemple, `use1-az1` il s'agit d'un identifiant AZ pour la `us-east-1` région et il a le même emplacement physique dans chaque région Compte AWS. L'illustration suivante montre comment les AZ IDs sont les mêmes pour tous les comptes, même si les noms des zones de disponibilité peuvent être mappés différemment pour chaque compte.



Avec S3 Express One Zone, vos données sont stockées de façon redondante sur plusieurs appareils au sein d'une même zone de disponibilité. S3 Express One Zone est conçu pour garantir une disponibilité de 99,95 % au sein d'une même zone de disponibilité et s'appuie sur le contrat de niveau de service Amazon S3. Pour de plus amples informations, consultez Zones de disponibilité.

Le tableau suivant montre les régions et les zones de disponibilité prises en charge par S3 Express One Zone :

Nom de la région	Code région	ID de zone de disponibilité				
USA Est (Virginie du Nord)	us-east-1	use1-az4				
		use1-az5				
		use1-az6				
USA Est (Ohio)	us-east-2	use2-az1				
		use2-az2				
USA Ouest (Oregon)	us-west-2	usw2-az1				
		usw2-az3				
		usw2-az4				
Asie-Pacifique (Mumbai)	ap-south-1	aps1-az1				
		aps1-az3				
Asie-Pacifique (Tokyo)	ap-northeast-1	apne1-az1				
		apne1-az4				
Europe (Irlande)	eu-west-1	euw1-az1				
		euw1-az3				
Europe (Stockholm)	eu-north-1	eun1-az1				
		eun1-az2				
		eun1-az3				

Mise en réseau des compartiments de répertoires dans une zone de disponibilité

Les rubriques suivantes décrivent les exigences de mise en réseau pour accéder à S3 Express One Zone à l'aide d'un point de terminaison de VPC de passerelle.

Rubriques

- Points de terminaison des compartiments de répertoires situés dans des zones de disponibilité
- Configuration de points de terminaison de VPC de passerelle

Points de terminaison des compartiments de répertoires situés dans des zones de disponibilité

Le tableau suivant indique les points de terminaison d'API régionaux et zonaux disponibles pour chaque région et zone de disponibilité.

Configuration de points de terminaison de VPC de passerelle

Utilisez la procédure suivante pour créer un point de terminaison de passerelle qui se connecte à des compartiments de répertoires et des objets de classe de stockage Amazon S3 Express One Zone.

Pour configurer un point de terminaison de VPC de passerelle

1. Ouvrez la console Amazon VPC.
2. Dans le volet de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Créez un nom pour votre point de terminaison.
5. Pour Service category (Catégorie de service), choisissez Services AWS.
6. Pour les services, ajoutez le filtre Type=Gateway, puis cliquez sur le bouton d'option à côté de com.amazonaws. ***region***.s3 express.
7. Pour VPC, choisissez le VPC dans lequel créer le point de terminaison.
8. Pour Configure route tables (Configurer les tables de routage), sélectionnez les tables de routage qui seront utilisées par le point de terminaison. Amazon VPC ajoute automatiquement une route pour pointer le trafic destiné au service vers l'interface réseau du point de terminaison.
9. Pour Politique, choisissez Accès complet afin d'autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, choisissez Personnalisé pour attacher une politique de point de terminaison de VPC qui contrôle les

autorisations dont disposent les principaux pour effectuer des actions sur les ressources via le point de terminaison de VPC.

10. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
11. Choisissez Créer un point de terminaison.

Après avoir créé un point de terminaison de passerelle, vous pouvez utiliser les points de terminaison d'API régionaux et les points de terminaison d'API zonaux pour accéder aux compartiments de répertoires et aux objets de classe de stockage Amazon S3 Express One Zone.

Création de compartiments de répertoires dans une zone de disponibilité

Pour commencer à utiliser la classe de stockage Amazon S3 Express One Zone, vous devez créer un compartiment de répertoires. La classe de stockage S3 Express One Zone peut être utilisée uniquement avec des compartiments de répertoires. Elle prend en charge les cas d'utilisation à faible latence et accélère le traitement des données au sein d'une même zone de disponibilité. Si votre application est sensible aux performances et peut bénéficier d'une latence inférieure à dix millisecondes pour les demandes `PUT` et `GET`, nous vous recommandons de créer un compartiment de répertoires afin de pouvoir utiliser la classe de stockage S3 Express One Zone.

Il existe deux types de compartiments Amazon S3 : les compartiments à usage général et les compartiments de répertoires. Vous devez choisir le type de compartiment qui correspond le mieux à votre application et à vos exigences de performances. Les compartiments à usage général constituent le type de compartiment S3 d'origine. Les compartiments à usage général sont recommandés pour la plupart des cas d'utilisation et des modèles d'accès. Ils autorisent le stockage d'objets dans toutes les classes de stockage, à l'exception de S3 Express One Zone. Pour plus d'informations sur les compartiments à usage général, consultez Présentation des compartiments à usage général.

Les compartiments de répertoires utilisent la classe de stockage S3 Express One Zone, conçue pour être utilisée pour les charges de travail ou les applications critiques en termes de performances qui nécessitent une latence constante inférieure à dix millisecondes. S3 Express One Zone est la première classe de stockage S3 dans laquelle vous pouvez sélectionner une zone de disponibilité unique avec la possibilité de regrouper le stockage d'objets et les ressources de calcul, ce qui assure la vitesse d'accès la plus élevée possible. Lorsque vous créez un bucket d'annuaire, vous pouvez éventuellement spécifier une zone de disponibilité Région AWS et une zone de disponibilité locales

pour vos instances de calcul Amazon EC2, Amazon Elastic Kubernetes Service ou Amazon Elastic Container Service (Amazon ECS) afin d'optimiser les performances.

Avec S3 Express One Zone, vos données sont stockées de façon redondante sur plusieurs appareils au sein d'une même zone de disponibilité. S3 Express One Zone est conçu pour garantir une disponibilité de 99,95 % au sein d'une même zone de disponibilité et s'appuie sur le contrat de niveau de service Amazon S3. Pour de plus amples informations, consultez Zones de disponibilité.

Les compartiments de répertoires organisent les données de manière hiérarchique dans des répertoires, contrairement à la structure de stockage horizontale des compartiments à usage général. Il n'existe pas de limite de préfixe pour les compartiments de répertoires et les répertoires individuels peuvent faire l'objet d'une mise à l'échelle horizontale.

Pour plus d'informations sur les compartiments de répertoires, consultez Utilisation des compartiments de répertoires.

Noms des compartiments de répertoires

Les noms des compartiments de répertoires doivent suivre ce format et respecter les règles de dénomination des compartiments de répertoires :

```
bucket-base-name--zone-id--x-s3
```

Par exemple, le nom de compartiment de répertoires suivant contient l'ID de zone de disponibilité `usw2-az1` :

```
bucket-base-name--usw2-az1--x-s3
```

Pour plus d'informations sur les règles de dénomination des compartiments de répertoires, consultez Règles de dénomination des compartiments de répertoires.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.

> **Note**
>
> Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste d'Amazon S3 Régions AWS, consultez la section sur les Service AWS points de terminaison dans le Référence générale d'Amazon Web Services.

3. Dans le volet de navigation de gauche, choisissez Directory buckets.
4. Choisissez Créer un compartiment. La page Créer un compartiment s'ouvre.
5. Sous Configuration générale, consultez l' Région AWS endroit où votre bucket sera créé.

   Sous Type de compartiment, choisissez Répertoire.

   > **Note**
   >
   > - Si vous avez choisi une région qui ne prend pas en charge les compartiments de répertoires, l'option Type de compartiment disparaît, et le type de compartiment est défini par défaut sur un compartiment à usage général. Pour créer un compartiment de répertoires, vous devez choisir une région prise en charge. Pour obtenir la liste des régions qui prennent en charge les compartiments de répertoires et la classe de stockage Amazon S3 Express One Zone, consultez the section called "Régions et zones de disponibilité S3 Express One Zone".
   > - Une fois que vous avez créé le compartiment, vous ne pouvez pas modifier son type.

   > **Note**
   >
   > La zone de disponibilité ne peut pas être modifiée une fois le compartiment créé.

6. Pour Zone de disponibilité, choisissez une zone de disponibilité locale pour vos services de calcul. Pour obtenir la liste des zones de disponibilité qui prennent en charge les compartiments de répertoires et la classe de stockage S3 Express One Zone, consultez the section called "Régions et zones de disponibilité S3 Express One Zone".

Sous Zone de disponibilité, cochez la case confirmant que vous comprenez qu'en cas de panne de la zone de disponibilité, vos données pourraient être indisponibles ou perdues.

> **Important**
>
> Les compartiments de répertoires sont stockés sur plusieurs appareils au sein d'une même zone de disponibilité, mais ne stockent pas les données de manière redondante entre les zones de disponibilité.

7. Pour Nom du compartiment, entrez un nom pour votre compartiment de répertoires.

   Les règles suivantes s'appliquent pour nommer les compartiments de répertoires :

   - Soyez unique au sein de la zone choisie (zone de AWS disponibilité ou zone AWS locale).
   - Le nom doit contenir entre 3 (minimum) et 63 caractères (maximum), suffixe inclus.
   - Doit être composé uniquement de lettres minuscules, de chiffres et de traits d'union (-).
   - Il doit commencer et se terminer par une lettre ou un chiffre.
   - Doit inclure le suffixe suivant : `--`*`zone-id`*`--x-s3`
   - Les noms de compartiment ne doivent pas commencer par le préfixe `xn--`.
   - Les noms de compartiment ne doivent pas commencer par le préfixe `sthree-`.
   - Les noms de compartiment ne doivent pas commencer par le préfixe `sthree-configurator`.
   - Les noms de compartiment ne doivent pas commencer par le préfixe `amzn-s3-demo-`.
   - Les noms de compartiment ne doivent pas se terminer par le suffixe `-s3alias`. Ce suffixe est réservé aux noms d'alias de point d'accès. Pour plus d'informations, consultez Alias de point d'accès.
   - Les noms de compartiment ne doivent pas se terminer par le suffixe `--ol-s3`. Ce suffixe est réservé aux noms d'alias de point d'accès Object Lambda. Pour de plus amples informations, veuillez consulter Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda de compartiment S3.
   - Les noms de compartiment ne doivent pas se terminer par le suffixe `.mrap`. Ce suffixe est réservé aux noms de point d'accès multi-régions. Pour de plus amples informations, veuillez consulter Règles relatives à l'attribution de noms pour les points d'accès multi-Régions Amazon S3.

Un suffixe est automatiquement ajouté au nom de base que vous fournissez lorsque vous créez un compartiment de répertoires à l'aide de la console. Ce suffixe inclut l'ID de la zone de disponibilité que vous avez choisie.

Une fois le compartiment créé, vous ne pouvez pas changer son nom. Pour plus d'informations sur l'attribution de noms à des compartiments, consultez Règles de dénomination des compartiments à usage général.

> **Important**
>
> N'ajoutez pas d'informations sensibles, notamment des numéros de compte, dans le nom du compartiment. Le nom du bucket est visible URLs là où pointent les objets du bucket.

8. Sous Propriété de l'objet, le paramètre imposé au propriétaire du compartiment est automatiquement activé et toutes les listes de contrôle d'accès (ACLs) sont désactivées. Impossible d'activer les ACLs compartiments de répertoire.

   Application par le propriétaire du compartiment (par défaut) : ACLs cette option est désactivée, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment à usage général et en a le contrôle total. ACLs n'affectent plus les autorisations d'accès aux données du compartiment à usage général S3. Le compartiment utilise des stratégies exclusivement pour définir le contrôle des accès.

9. Sous Paramètres de blocage de l'accès public pour ce compartiment, notez que les paramètres de blocage de l'accès public pour votre compartiment de répertoires sont automatiquement activés. Ces paramètres ne peuvent pas être modifiés pour les compartiments de répertoires. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

10. Pour configurer le chiffrement par défaut, dans Type de chiffrement, choisissez l'une des options suivantes :

    - Chiffrement côté serveur avec clé gérée Amazon S3 (SSE-S3)
    - Chiffrement côté serveur avec AWS Key Management Service clé (SSE-KMS)

    Pour en savoir plus sur l'utilisation du chiffrement côté serveur Amazon S3 pour chiffrer vos données, consultez Protection et chiffrement des données.

> **Important**
>
> Si vous utilisez l'option SSE-KMS pour votre configuration de chiffrement par défaut, vous êtes soumis aux quotas RPS (demandes par seconde) de AWS KMS. Pour plus d'informations sur les quotas de AWS KMS et sur la procédure à suivre pour demander une augmentation des quotas, consultez Quotas dans le Guide du développeur AWS Key Management Service .
> Lorsque vous activez le chiffrement par défaut, vous devrez peut-être mettre à jour votre politique de compartiment. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement SSE-KMS pour les opérations intercomptes.

11. Si vous avez choisi le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), sous Bucket Key, Enabled apparaît. Les clés de compartiment S3 sont toujours activées lorsque vous configurez votre compartiment d'annuaire pour utiliser le chiffrement par défaut avec SSE-S3. Les clés de compartiment S3 sont toujours activées pour les opérations `GET` et `PUT` dans un compartiment de répertoires et ne peuvent pas être désactivées. Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de CopyObject, d'UploadPartCopy, de l'opération Copy dans les opérations par lot ou des tâches import. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS.

    Les clés de compartiment S3 réduisent le coût du chiffrement en diminuant le trafic de demandes d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

12. Si vous avez choisi le chiffrement côté serveur avec AWS Key Management Service clé (SSE-KMS), sous AWS KMS clé, spécifiez votre AWS Key Management Service clé de l'une des manières suivantes ou créez-en une nouvelle.

    - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans Disponible AWS KMS keys.

      Seules les clés gérées par vos clients apparaissent dans cette liste. Le Clé gérée par AWS (`aws/s3`) n'est pas pris en charge dans les compartiments de répertoire. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

- Pour saisir l'ARN ou l'alias de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN ou l'alias de votre clé KMS dans AWS KMS key ARN.
- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

  Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> - Votre configuration SSE-KMS ne peut prendre en charge qu'une seule clé gérée par le client par compartiment de répertoires pendant toute la durée de vie du compartiment. La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. De même, après avoir spécifié une clé gérée par le client pour SSE-KMS, vous ne pouvez pas remplacer la clé gérée par le client pour la configuration SSE-KMS du compartiment.
>
>   Vous pouvez identifier la clé gérée par le client que vous avez spécifiée pour la configuration SSE-KMS du compartiment de la manière suivante :
>
>   - Effectuez une demande d'opération d'API `HeadObject` pour trouver la valeur de `x-amz-server-side-encryption-aws-kms-key-id` dans la réponse.
>
>   Pour utiliser une nouvelle clé gérée par le client pour vos données, nous vous recommandons de copier vos objets existants dans un nouveau compartiment de répertoires avec une nouvelle clé gérée par le client.
> - Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez d'abord avoir l'autorisation d'utiliser cette clé, puis vous devez saisir l'ARN de la clé KMS. Pour plus d'informations sur les autorisations entre comptes pour les clés KMS, consultez Création de clés KMS que d'autres comptes peuvent utiliser dans le Guide du développeur AWS Key Management Service . Pour en savoir plus sur SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) pour les chargements de nouveaux objets dans des compartiments de répertoires.

- Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans des compartiments de répertoire, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez Identification des clés KMS symétriques et asymétriques dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur l'utilisation AWS KMS avec Amazon S3, consultezUtilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de répertoire.

13. Choisissez Créer un compartiment. Après avoir créé le compartiment, vous pouvez y ajouter des fichiers et des dossiers. Pour de plus amples informations, veuillez consulter the section called "Utilisation d'objets dans un compartiment de répertoires".

À l'aide du AWS SDKs

SDK for Go

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit AWS SDK pour Go.

Example

```
var bucket = "..."

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("usw2-az1"),
                Type: types.LocationTypeAvailabilityZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleAvailabilityZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
```

```
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n")
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit AWS SDK for Java 2.x.

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{az-id}--x-s3
    //example: doc-example-bucket--usw2-az1--x-s3 is a valid name for a directory
 bucket created in
    //Region us-west-2, Availability Zone 2

    CreateBucketConfiguration bucketConfiguration =
 CreateBucketConfiguration.builder()
            .location(LocationInfo.builder()
                    .type(LocationType.AVAILABILITY_ZONE)
                    .name("usw2-az1").build()) //this must match the Region and
 Availability Zone in your bucket name
            .bucket(BucketInfo.builder()
                   .type(BucketType.DIRECTORY)
                   .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
                   .build()).build();
    try {

            CreateBucketRequest bucketRequest =
 CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
            CreateBucketResponse response = s3Client.createBucket(bucketRequest);
            System.out.println(response);
```

```
    }

    catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
         }
    }
```

AWS SDK pour JavaScript

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit AWS SDK pour JavaScript.

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "us-east-1";
const zone = "use1-az4";
const suffix = `${zone}--x-s3`;

const s3 = new S3({ region });

const bucketName = `...--${suffix}`;

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "AvailabilityZone", Name: zone},
      Bucket: { Type: "Directory", DataRedundancy: "SingleAvailabilityZone" }}
    }
   );
```

SDK pour .NET

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit SDK pour .NET.

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

       BucketName = "DOC-EXAMPLE-BUCKET--usw2-az1--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
       {
         BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleAvailabilityZone, Type = BucketType.Directory },
         Location = new LocationInfo { Name = "usw2-az1", Type =
 LocationType.AvailabilityZone }
       }
     }).ConfigureAwait(false);
}
```

SDK for PHP

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit AWS SDK for PHP.

Example

```
require 'vendor/autoload.php';

$s3Client = new S3Client([

    'region'      => 'us-east-1',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'doc-example-bucket--use1-az4--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'use1-az4', 'Type'=> 'AvailabilityZone'],
        'Bucket' => ["DataRedundancy" => "SingleAvailabilityZone" ,"Type" =>
 "Directory"]   ],
]);
```

SDK for Python

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit AWS SDK pour Python (Boto3).

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, availability_zone):
    '''
    Create a directory bucket in a specified Availability Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :param availability_zone: String; Availability Zone ID to create the bucket in,
 for example, 'usw2-az1'
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'AvailabilityZone',
                    'Name': availability_zone
                },
                'Bucket': {
                    'Type': 'Directory',
                    'DataRedundancy': 'SingleAvailabilityZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True
```

```
if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    availability_zone = 'usw2-az1'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, availability_zone)
```

SDK for Ruby

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit AWS SDK pour Ruby.

Example

```
s3 = Aws::S3::Client.new(region:'us-west-2')
s3.create_bucket(
  bucket: "bucket_base_name--az_id--x-s3",
  create_bucket_configuration: {
    location: { name: 'usw2-az1', type: 'AvailabilityZone' },
    bucket: { data_redundancy: 'SingleAvailabilityZone', type: 'Directory' }
  }
)
```

À l'aide du AWS CLI

Cet exemple montre comment créer un compartiment de répertoires à l'aide du kit AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Lorsque vous créez un compartiment de répertoires, vous devez fournir les détails de configuration et utiliser la convention de dénomination suivante : *bucket-base-name*--*zone-id*--x-s3

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=AvailabilityZone,Name=usw2-
az1},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory}'
--region us-west-2
```

Pour plus d'informations, consultez create-bucket dans l' AWS Command Line Interface.

Points de terminaison régionaux et zonaux pour les compartiments de répertoires d'une zone de disponibilité

Pour accéder aux objets et aux compartiments de répertoires stockés dans S3 Express One Zone, utilisez des points de terminaison de VPC de passerelle. Les compartiments de répertoires utilisent des points de terminaison d'API régionaux et zonaux. Selon l'opération d'API Amazon S3 que vous utilisez, un point de terminaison régional ou zonal est requis. Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle.

Les opérations d'API de niveau compartiment (ou plan de contrôle) sont disponibles via les points de terminaison régionaux et sont appelées opérations d'API de point de terminaison régional. `CreateBucket` et `DeleteBucket` sont des exemples d'opérations d'API de point de terminaison régional.

Lorsque vous créez des compartiments de répertoires stockés dans S3 Express One Zone, vous choisissez la zone de disponibilité dans laquelle le compartiment figurera. Vous pouvez utiliser les opérations d'API de point de terminaison zonal pour charger et gérer les objets dans votre compartiment de répertoires.

Les opérations d'API de niveau objet (ou plan de données) sont disponibles via les points de terminaison zonaux et sont appelées opérations d'API de point de terminaison zonal. `CreateSession` et `PutObject` sont des exemples d'opérations d'API de point de terminaison zonal.

Optimisation des performances de S3 Express One Zone

Amazon S3 Express One Zone est une classe de stockage S3 à zone de disponibilité (AZ) unique, à hautes performances, spécialement conçue pour fournir un accès aux données constant en moins de dix millisecondes pour vos applications les plus sensibles à la latence. S3 Express One Zone est la première classe de stockage S3 qui vous permet de regrouper des ressources de AWS calcul et de stockage d'objets hautes performances, telles qu'Amazon Elastic Compute Cloud, Amazon Elastic Kubernetes Service et Amazon Elastic Container Service, au sein d'une seule zone de disponibilité. Le regroupement des ressources de stockage et de calcul optimise les performances et les coûts de calcul et augmente la vitesse de traitement des données.

S3 Express One Zone offre une élasticité des performances similaire à celle des autres classes de stockage S3, mais avec des latences du premier octet constantes de demande de lecture et d'écriture en moins de dix millisecondes, jusqu'à 10 fois plus rapides que S3 Standard. S3 Express One Zone est entièrement conçu pour prendre en charge un débit en rafale jusqu'à des niveaux

d'agrégation très élevés. La classe de stockage S3 Express One Zone utilise une architecture personnalisée pour optimiser les performances et garantir une faible latence des demandes en stockant les données sur du matériel à hautes performances. Le protocole d'objet pour S3 Express One Zone a été amélioré afin de rationaliser l'authentification et la surcharge de métadonnées.

Pour réduire davantage la latence et prendre en charge jusqu'à 2 millions de lectures et jusqu'à 200 000 écritures par seconde, S3 Express One Zone stocke les données dans un compartiment d'annuaire Amazon S3. Par défaut, chaque compartiment de répertoire prend en charge jusqu'à 200 000 lectures et 100 000 écritures par seconde. Si votre charge de travail nécessite des limites TPS supérieures aux limites par défaut, vous pouvez demander une augmentation par le biais du AWS Support.

La combinaison d'un matériel et de logiciels spécialement conçus à hautes performances, offrant une vitesse d'accès aux données de l'ordre de quelques millisecondes, et de compartiments de répertoires pouvant être mis à l'échelle pour un grand nombre de transactions par seconde fait de S3 Express One Zone la meilleure classe de stockage Amazon S3 pour les opérations exigeantes en termes de demandes ou les applications critiques en matière de performances.

Les rubriques suivantes décrivent les bonnes pratiques à suivre et les modèles de conception pour optimiser les performances des applications qui utilisent la classe de stockage S3 Express One Zone.

Rubriques

- Meilleures pratiques pour optimiser les performances de S3 Express One Zone

Meilleures pratiques pour optimiser les performances de S3 Express One Zone

Lors du développement d'applications qui chargent et récupèrent les objets depuis Amazon S3 Express One Zone, suivez nos bonnes pratiques pour optimiser les performances. Pour utiliser la classe de stockage S3 Express One Zone, vous devez créer un compartiment de répertoires S3. La classe de stockage S3 Express One Zone n'est pas prise en charge pour une utilisation avec les compartiments S3 à usage général.

Pour accéder aux directives d'optimisation des performances relatives à toutes les autres classes de stockage Amazon S3 et aux compartiments à usage général S3, consultez Modèles de conception des bonnes pratiques : optimisation des performances d'Amazon S3.

Pour optimiser les performances et l'évolutivité de la classe de stockage S3 Express One Zone et des compartiments de répertoire pour les charges de travail à grande échelle, il est important de

comprendre en quoi les compartiments de répertoire fonctionnent différemment des compartiments à usage général. Ensuite, nous proposons les meilleures pratiques pour aligner vos applications sur le fonctionnement des buckets d'annuaires.

Comment fonctionnent les compartiments de répertoires

La classe de stockage Amazon S3 Express One Zone peut prendre en charge des charges de travail comportant jusqu'à 2 000 000 de transactions GET et jusqu'à 200 000 transactions PUT par seconde (TPS) par compartiment de répertoire. Avec S3 Express One Zone, les données sont stockées dans des compartiments de répertoire S3 situés dans des zones de disponibilité. Les objets des compartiments de répertoire sont accessibles dans un espace de noms hiérarchique, comme dans un système de fichiers, contrairement aux compartiments à usage général S3 dotés d'un espace de noms plat. Contrairement aux compartiments à usage général, les compartiments de répertoires organisent les clés de manière hiérarchique dans des répertoires plutôt qu'avec des préfixes. Un préfixe est une chaîne de caractères au début du nom de la clé d'objet. Vous pouvez utiliser des préfixes pour organiser vos données et gérer une architecture de stockage d'objets plats dans des compartiments à usage général. Pour de plus amples informations, veuillez consulter Organisation des objets à l'aide de préfixes.

Dans les compartiments de répertoire, les objets sont organisés dans un espace de noms hiérarchique en utilisant forward slash (`/`) comme seul séparateur pris en charge. Lorsque vous chargez un objet avec une clé telle que`dir1/dir2/file1.txt`, les répertoires `dir1/` `dir2/` sont automatiquement créés et gérés par Amazon S3. Les répertoires sont créés pendant `PutObject` `CreateMultiPartUpload` les opérations et automatiquement supprimés lorsqu'ils deviennent vides après `DeleteObject` `AbortMultiPartUpload` les opérations. Il n'y a pas de limite supérieure au nombre d'objets et de sous-répertoires dans un répertoire.

Les répertoires créés lorsque les objets sont chargés dans des compartiments de répertoires peuvent être redimensionnés instantanément afin de réduire le risque d'erreurs HTTP. `503 (Slow Down)` Cette mise à l'échelle automatique permet à vos applications de mettre en parallèle les demandes de lecture et d'écriture dans et entre les répertoires, selon les besoins. Pour S3 Express One Zone, les annuaires individuels sont conçus pour prendre en charge le taux de requêtes maximal d'un bucket de répertoires. Il n'est pas nécessaire de randomiser les préfixes de clé pour obtenir des performances optimales, car le système distribue automatiquement les objets pour une répartition uniforme de la charge. Par conséquent, les clés ne sont pas stockées lexicographiquement dans des compartiments de répertoire. Cela contraste avec les compartiments à usage général S3 où les clés les plus proches du point de vue lexicographique sont plus susceptibles d'être colocalisées sur le même serveur.

Pour plus d'informations sur des exemples d'opérations de bucket d'annuaire et d'interactions d'annuaires, consultezExemples d'opérations de bucket et d'interactions entre annuaires.

Bonnes pratiques

Suivez les meilleures pratiques pour optimiser les performances de votre bucket d'annuaires et faire évoluer vos charges de travail au fil du temps.

Utilisez des répertoires contenant de nombreuses entrées (objets ou sous-répertoires)

Les compartiments d'annuaire offrent des performances élevées par défaut pour toutes les charges de travail. Pour optimiser encore les performances de certaines opérations, la consolidation d'un plus grand nombre d'entrées (objets ou sous-répertoires) dans des répertoires réduira le temps de latence et augmentera le taux de requêtes :

- Les opérations d'API mutantes, telles que`PutObject`, `CreateMultiPartUpload` et `DeleteObjectAbortMultiPartUpload`, permettent d'obtenir des performances optimales lorsqu'elles sont mises en œuvre avec des répertoires moins nombreux et plus denses contenant des milliers d'entrées, plutôt qu'avec un grand nombre de répertoires plus petits.
- `ListObjectsV2`les opérations sont plus performantes lorsque moins de répertoires doivent être parcourus pour remplir une page de résultats.

N'utilisez pas l'entropie dans les préfixes

Dans les opérations Amazon S3, l'entropie fait référence au caractère aléatoire de la dénomination des préfixes qui permet de répartir les charges de travail de manière uniforme sur les partitions de stockage. Cependant, étant donné que les compartiments de répertoire gèrent en interne la distribution de la charge, il n'est pas recommandé d'utiliser l'entropie dans les préfixes pour de meilleures performances. En effet, pour les compartiments de répertoires, l'entropie peut ralentir les demandes en ne réutilisant pas les répertoires déjà créés.

Un modèle clé tel que celui-ci `$HASH/directory/object` pourrait finir par créer de nombreux répertoires intermédiaires. Dans l'exemple suivant, tous les `job-1` s sont des répertoires différents puisque leurs parents sont différents. Les répertoires seront rares et les demandes de mutation et de liste seront plus lentes. Dans cet exemple, il existe 12 répertoires intermédiaires qui ont tous une seule entrée.

```
s3://my-bucket/0cc175b9c0f1b6a831c399e269772661/job-1/file1
```

```
s3://my-bucket/92eb5ffee6ae2fec3ad71c777531578f/job-1/file2

s3://my-bucket/4a8a08f09d37b73795649038408b5f33/job-1/file3

s3://my-bucket/8277e0910d750195b448797616e091ad/job-1/file4

s3://my-bucket/e1671797c52e15f763380b45e841ec32/job-1/file5

s3://my-bucket/8fa14cdd754f91cc6554c9e71929cce7/job-1/file6
```

Au lieu de cela, pour de meilleures performances, nous pouvons supprimer le $HASH composant et l'autoriser `job-1` à devenir un répertoire unique, améliorant ainsi la densité d'un répertoire. Dans l'exemple suivant, le répertoire intermédiaire unique comportant 6 entrées peut améliorer les performances par rapport à l'exemple précédent.

```
s3://my-bucket/job-1/file1

s3://my-bucket/job-1/file2

s3://my-bucket/job-1/file3

s3://my-bucket/job-1/file4

s3://my-bucket/job-1/file5

s3://my-bucket/job-1/file6
```

Cet avantage en termes de performances est dû au fait que lorsqu'une clé d'objet est initialement créée et que son nom de clé inclut un répertoire, celui-ci est automatiquement créé pour l'objet. Les chargements d'objets ultérieurs vers ce même répertoire ne nécessitent pas la création du répertoire, ce qui réduit la latence lors des chargements d'objets vers les répertoires existants.

Utilisez un séparateur autre que le délimiteur/pour séparer les parties de votre clé si vous n'avez pas besoin de pouvoir regrouper des objets de manière logique pendant les appels **`ListObjectsV2`**

Étant donné que le `/` délimiteur est traité spécialement pour les compartiments de répertoires, il doit être utilisé avec intention. Bien que les compartiments de répertoire n'ordonnent pas les objets de manière lexicographique, les objets d'un répertoire sont toujours regroupés dans les sorties. `ListObjectsV2` Si vous n'avez pas besoin de cette fonctionnalité, vous pouvez le `/` remplacer par un autre caractère comme séparateur afin de ne pas provoquer la création de répertoires intermédiaires.

Supposons, par exemple, que les clés suivantes suivent un modèle de YYYY/MM/DD/HH/ préfixe

```
s3://my-bucket/2024/04/00/01/file1

s3://my-bucket/2024/04/00/02/file2

s3://my-bucket/2024/04/00/03/file3

s3://my-bucket/2024/04/01/01/file4

s3://my-bucket/2024/04/01/02/file5

s3://my-bucket/2024/04/01/03/file6
```

Si vous n'avez pas besoin de regrouper les objets par heure ou par jour dans les `ListObjectsV2` résultats, mais que vous devez regrouper les objets par mois, le schéma clé suivant `YYYY/MM/DD-HH-` permettra de réduire considérablement le nombre de répertoires et d'améliorer les performances de l'`ListObjectsV2`opération.

```
s3://my-bucket/2024/04/00-01-file1

s3://my-bucket/2024/04/00-01-file2

s3://my-bucket/2024/04/00-01-file3

s3://my-bucket/2024/04/01-02-file4

s3://my-bucket/2024/04/01-02-file5

s3://my-bucket/2024/04/01-02-file6
```

Utilisez des opérations de liste délimitées dans la mesure du possible

Une `ListObjectsV2` requête dépourvue de `delimiter` effectue une traversée récursive de tous les répertoires en fonction de la profondeur d'abord. Une `ListObjectsV2` requête contenant un `delimiter` extrait uniquement les entrées du répertoire spécifié par le `prefix` paramètre, ce qui réduit le temps de latence des demandes et augmente le nombre de clés agrégées par seconde. Pour les compartiments de répertoire, utilisez des opérations de liste délimitées dans la mesure du possible. Les listes délimitées réduisent le nombre de visites dans les annuaires, ce qui se traduit par un plus grand nombre de clés par seconde et une latence des demandes plus faible.

Par exemple, pour les répertoires et objets suivants de votre bucket de répertoire :

```
s3://my-bucket/2024/04/12-01-file1

s3://my-bucket/2024/04/12-01-file2

...

s3://my-bucket/2024/05/12-01-file1

s3://my-bucket/2024/05/12-01-file2

...

s3://my-bucket/2024/06/12-01-file1

s3://my-bucket/2024/06/12-01-file2

...

s3://my-bucket/2024/07/12-01-file1

s3://my-bucket/2024/07/12-01-file2

...
```

Pour de meilleures `ListObjectsV2` performances, utilisez une liste délimitée pour répertorier vos sous-répertoires et vos objets, si la logique de votre application le permet. Par exemple, vous pouvez exécuter la commande suivante pour l'opération de liste délimitée :

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/' --delimiter '/'
```

Le résultat est la liste des sous-répertoires.

```
{
    "CommonPrefixes": [
        {
            "Prefix": "2024/04/"
        },
        {
            "Prefix": "2024/05/"
        },
```

```
        {
            "Prefix": "2024/06/"
        },
        {
            "Prefix": "2024/07/"
        }
    ]
}
```

Pour répertorier chaque sous-répertoire avec de meilleures performances, vous pouvez exécuter une commande comme dans l'exemple suivant :

Commande :

```
aws s3api list-objects-v2 --bucket my-bucket --prefix '2024/04' --delimiter '/'
```

Sortie :

```
{
    "Contents": [
        {
            "Key": "2024/04/12-01-file1"
        },
        {
            "Key": "2024/04/12-01-file2"
        }
    ]
}
```

Regroupement du stockage S3 Express One Zone et de vos ressources de calcul

Avec S3 Express One Zone, chaque compartiment de répertoire est situé dans une seule zone de disponibilité que vous sélectionnez lorsque vous créez le compartiment. Vous pouvez commencer par créer un nouveau compartiment de répertoires dans une zone de disponibilité locale pour vos charges de travail ou vos ressources de calcul. Vous pouvez alors commencer immédiatement des opérations de lecture et d'écriture à très faible latence. Les compartiments de répertoire sont un type de compartiments S3 dans lesquels vous pouvez choisir la zone de disponibilité dans un Région AWS afin de réduire le temps de latence entre le calcul et le stockage.

Si vous accédez à des compartiments d'annuaire à travers des zones de disponibilité, il est possible que vous rencontriez une légère augmentation de la latence. Pour optimiser les performances, nous

vous recommandons d'accéder à un compartiment de répertoires depuis des instances Amazon Elastic Container Service, Amazon Elastic Kubernetes Service et Amazon Elastic Compute Cloud situées dans la même zone de disponibilité, quand cela est possible.

Utilisez des connexions simultanées pour atteindre un débit élevé avec des objets de plus de 1 Mo

Vous pouvez optimiser les performances en adressant plusieurs demandes simultanées aux compartiments de répertoires pour répartir vos demandes sur des connexions distinctes et augmenter au maximum la bande passante accessible. À l'instar des compartiments à usage général, S3 Express One Zone n'impose aucune limite quant au nombre de connexions établies avec votre compartiment d'annuaire. Les répertoires individuels peuvent mettre à l'échelle horizontalement et automatiquement les performances quand un grand nombre d'écritures simultanées sont effectuées dans le même répertoire.

Les connexions TCP individuelles aux compartiments de répertoire ont une limite supérieure fixe pour le nombre d'octets pouvant être chargés ou téléchargés par seconde. Lorsque les objets grossissent, les temps de requête sont dominés par le streaming d'octets plutôt que par le traitement des transactions. Pour utiliser plusieurs connexions afin de paralléliser le chargement ou le téléchargement d'objets plus volumineux, vous pouvez réduire end-to-end le temps de latence. Si vous utilisez le `Java 2.x` SDK, vous devriez envisager d'utiliser le S3 Transfer Manager, qui bénéficiera des améliorations de performances, telles que les opérations d'API de téléchargement partitionné et les extractions par plage d'octets pour accéder aux données en parallèle.

Utiliser les points de terminaison VPC Gateway

Les points de terminaison de passerelle fournissent une connexion directe entre votre VPC et les compartiments de répertoire, sans nécessiter de passerelle Internet ou de périphérique NAT pour votre VPC. Pour réduire le temps que vos paquets passent sur le réseau, vous devez configurer votre VPC avec un point de terminaison VPC passerelle pour les compartiments de répertoire. Pour de plus amples informations, veuillez consulter Mise en réseau des compartiments de répertoires.

Utilisez l'authentification de session et réutilisez les jetons de session lorsqu'ils sont valides

Les compartiments d'annuaire fournissent un mécanisme d'authentification par jeton de session pour réduire la latence lors des opérations d'API sensibles aux performances. Vous pouvez passer un seul appel pour `CreateSession` obtenir un jeton de session qui sera ensuite valide pour toutes les demandes dans les 5 minutes suivantes. Pour réduire au maximum la latence de vos appels d'API, assurez-vous d'acquérir un jeton de session et de le réutiliser pendant toute la durée de vie de ce jeton avant de l'actualiser.

Si vous l'utilisez AWS SDKs, SDKs gérez automatiquement les actualisations des jetons de session afin d'éviter les interruptions de service à l'expiration d'une session. Nous vous recommandons d'utiliser le AWS SDKs pour lancer et gérer les demandes relatives à l'opération `CreateSession` API.

Pour plus d'informations sur `CreateSession`, consultez Autorisation des opérations d'API de point de terminaison zonal avec `CreateSession`.

Utiliser un client CRT

Le AWS Common Runtime (CRT) est un ensemble de bibliothèques modulaires, performantes et efficaces écrites en C et destinées à servir de base au AWS SDKs. Le CRT fournit un débit amélioré, une meilleure gestion des connexions et des temps de démarrage plus rapides. Le CRT est disponible sur tous les réseaux AWS SDKs sauf Go.

Pour plus d'informations sur la configuration du CRT pour le SDK que vous utilisez, consultez les bibliothèques AWS Common Runtime (CRT), Accélérez le débit d'Amazon S3 avec le AWS Common Runtime, Présentation duclient S3 basé sur CRT et du gestionnaire de transfert S3 dans le SDK pour Java AWS 2.x, Utilisation de S3 pour les opérations CrtClient Amazon S3 et Configuration des clients HTTP basés sur le CRT. AWS

Utilisez la dernière version du AWS SDKs

Ils AWS SDKs fournissent un support intégré pour de nombreuses directives recommandées pour optimiser les performances d'Amazon S3. Ils SDKs proposent une API plus simple pour tirer parti d'Amazon S3 depuis une application et sont régulièrement mis à jour pour suivre les meilleures pratiques les plus récentes. Par exemple, ils réessayent SDKs automatiquement les demandes après des `503` erreurs HTTP et gèrent les réponses lentes aux connexions.

Si vous utilisez le `Java 2.x` SDK, vous devriez envisager d'utiliser le gestionnaire de transfert S3, qui redimensionne automatiquement les connexions horizontalement pour traiter des milliers de demandes par seconde en utilisant des requêtes par plage d'octets, le cas échéant. Les requêtes par plage d'octets peuvent améliorer les performances car vous pouvez utiliser des connexions simultanées à S3 pour récupérer différentes plages d'octets au sein d'un même objet. Vous pouvez ainsi parvenir au regroupement de débits le plus élevé, par opposition à une seule demande d'objet entier. Il est donc important d'utiliser la dernière version du AWS SDKs pour obtenir les dernières fonctionnalités d'optimisation des performances.

Dépannage des performances

Configurez-vous des demandes de nouvelle tentative pour les applications sensibles à la latence ?

La classe S3 Express One Zone est spécialement conçue pour fournir des niveaux élevés constants de performances sans réglages supplémentaires. Toutefois, la définition de valeurs de délai d’attente et de nouvelles tentatives agressives contribue également à garantir une latence et des performances constantes. Ils AWS SDKs ont des valeurs de délai d'expiration et de nouvelle tentative configurables que vous pouvez ajuster en fonction des tolérances de votre application spécifique.

Utilisez-vous des bibliothèques CRT (AWS Common Runtime) et des types d' EC2 instances Amazon optimaux ?

Les applications qui effectuent un grand nombre d’opérations de lecture et d’écriture ont probablement besoin de plus de mémoire et de capacité de calcul que les autres. Lorsque vous lancez vos instances Amazon Elastic Compute Cloud (Amazon EC2) pour votre charge de travail exigeante en performances, choisissez des types d'instances dotés de la quantité de ressources dont votre application a besoin. Le stockage hautes performances S3 Express One Zone est idéalement associé à des types d'instances plus grands et plus récents, dotés d'une plus grande quantité de mémoire système et plus puissants, CPUs et GPUs qui peuvent tirer parti d'un stockage plus performant. Nous recommandons également d'utiliser les dernières versions de la technologie compatible CRT AWS SDKs, qui permettent de mieux accélérer les requêtes de lecture et d'écriture en parallèle.

Utilisez-vous une authentification basée sur AWS SDKs les sessions ?

Avec Amazon S3, vous pouvez également optimiser les performances lorsque vous utilisez des requêtes d'API HTTP REST en suivant les mêmes bonnes pratiques que celles décrites dans le AWS SDKs. Toutefois, compte tenu du mécanisme d'autorisation et d'authentification basé sur les sessions utilisé par S3 Express One Zone, nous vous recommandons vivement d'utiliser le AWS SDKs to manage `CreateSession` et son jeton de session géré. Créez et actualisez AWS SDKs automatiquement les jetons en votre nom à l'aide de l'opération `CreateSession` API. Utilisation d'`CreateSession`économies sur le temps de latence aller-retour par demande vers AWS Identity and Access Management (IAM) pour autoriser chaque demande.

Exemples d'opérations de bucket et d'interactions entre annuaires

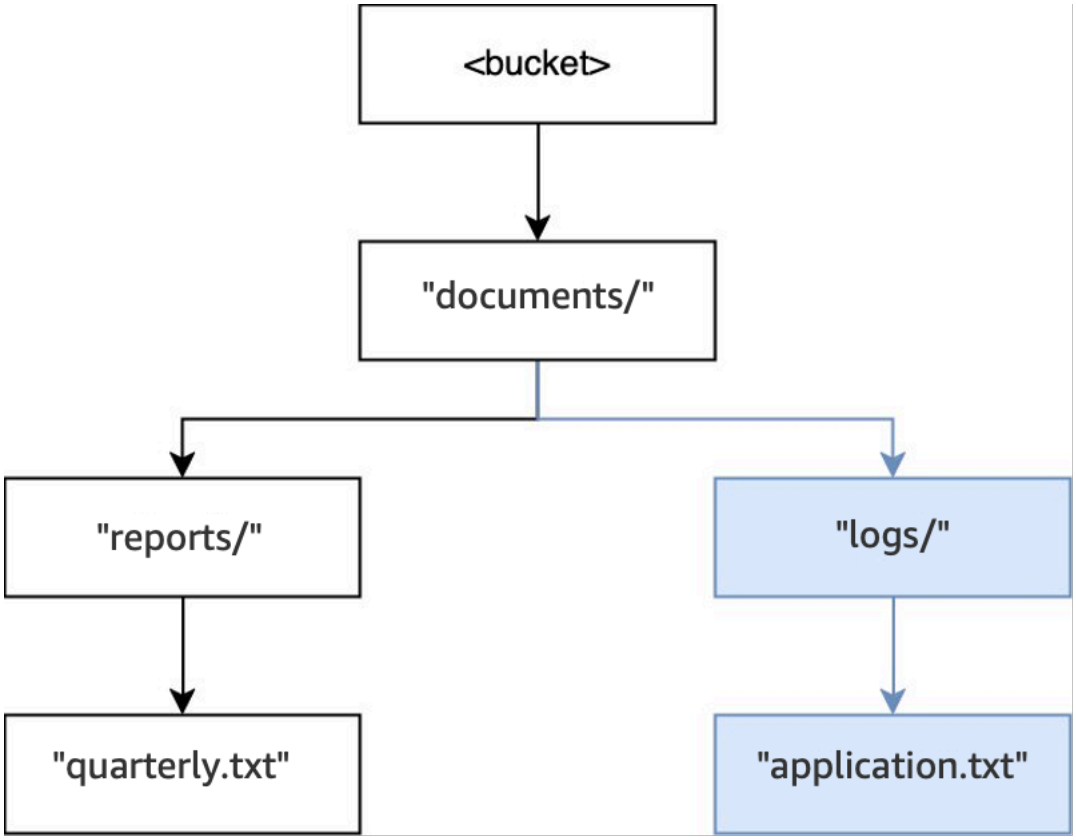
Voici trois exemples illustrant le fonctionnement des compartiments de répertoire.

Exemple 1 : Comment les **`PutObject`** requêtes S3 adressées à un compartiment de répertoire interagissent avec les annuaires

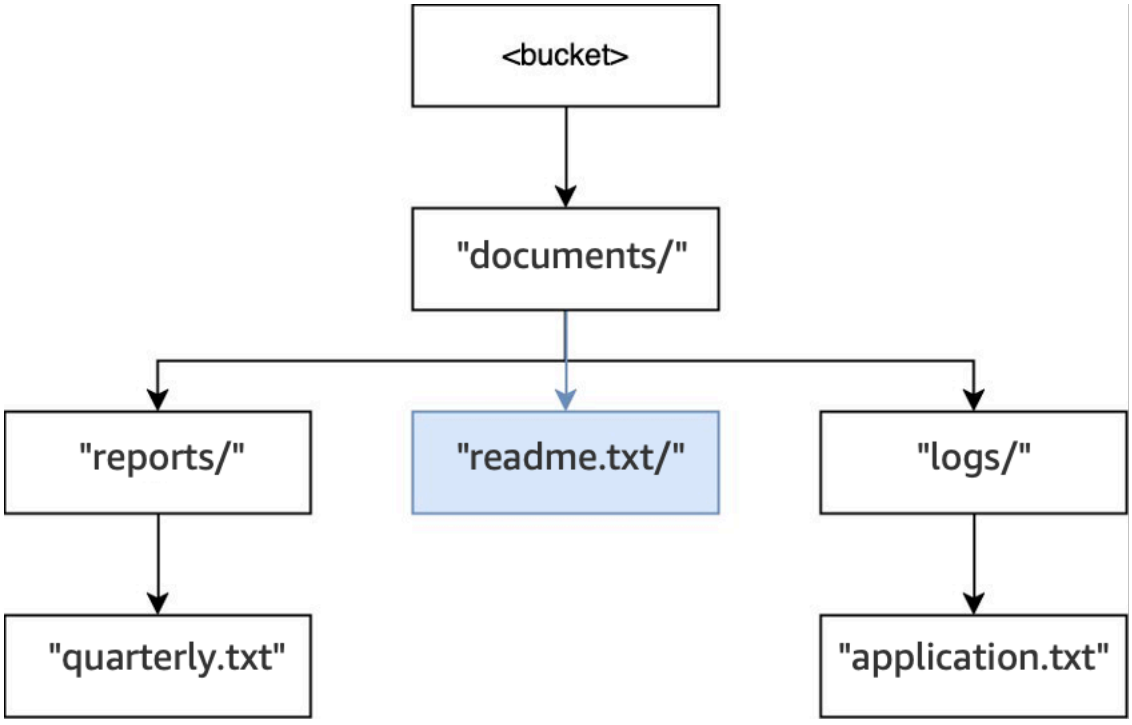
1. Lorsque l'opération `PUT(<bucket>, "documents/reports/quarterly.txt")` est exécutée dans un compartiment vide, le répertoire `documents/` situé à la racine du compartiment est créé, le répertoire situé à l'`reports/`intérieur `documents/` est créé et l'objet qu'`reports/`il `quarterly.txt` contient est créé. Pour cette opération, deux répertoires ont été créés en plus de l'objet.



2. Ensuite, lorsqu'une autre opération `PUT(<bucket>, "documents/logs/application.txt")` est exécutée, le répertoire existe `documents/` déjà, le `logs/` répertoire qu'il contient `documents/` n'existe pas et est créé, et l'objet qu'`logs/`il `application.txt` contient est créé. Pour cette opération, un seul répertoire a été créé en plus de l'objet.



3. Enfin, lorsqu'une `PUT(<bucket>, "documents/readme.txt")` opération est exécutée, le répertoire situé `documents/` dans la racine existe déjà et l'objet `readme.txt` est créé. Pour cette opération, aucun répertoire n'est créé.



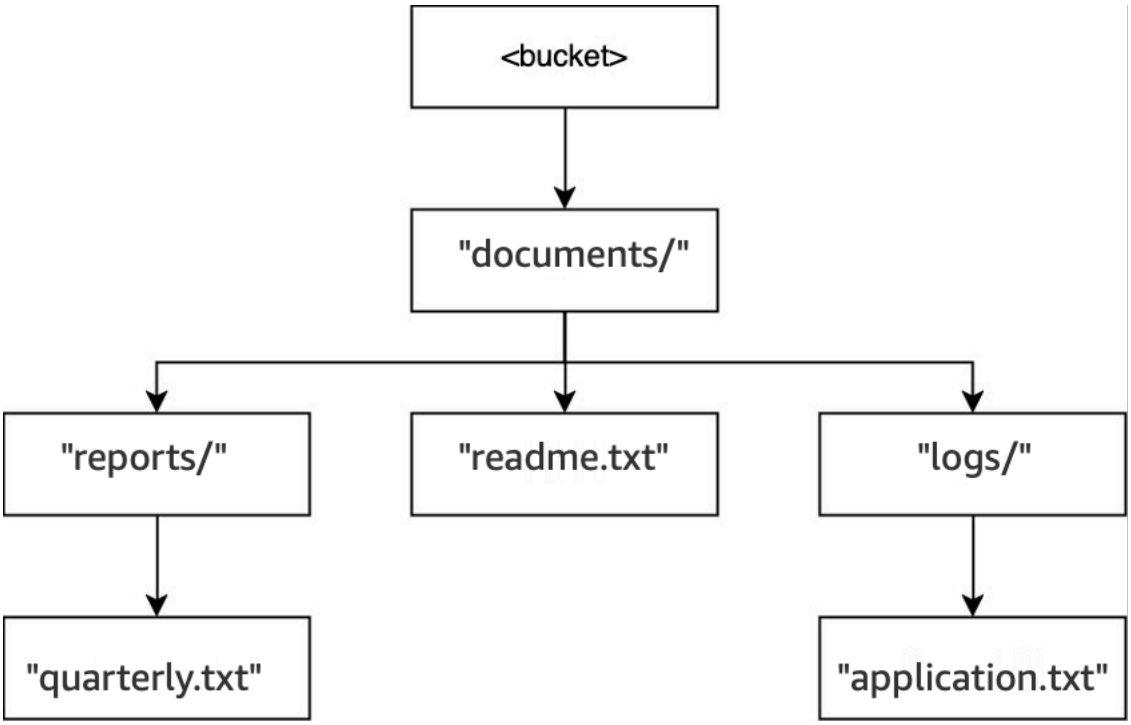
Exemple 2 : Comment les **`ListObjectsV2`** requêtes S3 adressées à un compartiment de répertoire interagissent avec les annuaires

Pour les `ListObjectsV2` demandes S3 sans spécifier de délimiteur, un compartiment est parcouru en fonction de la profondeur d'abord. Les sorties sont renvoyées dans un ordre cohérent. Cependant, bien que cet ordre reste le même entre les demandes, il n'est pas lexicographique. Pour le bucket et les répertoires créés dans l'exemple précédent :

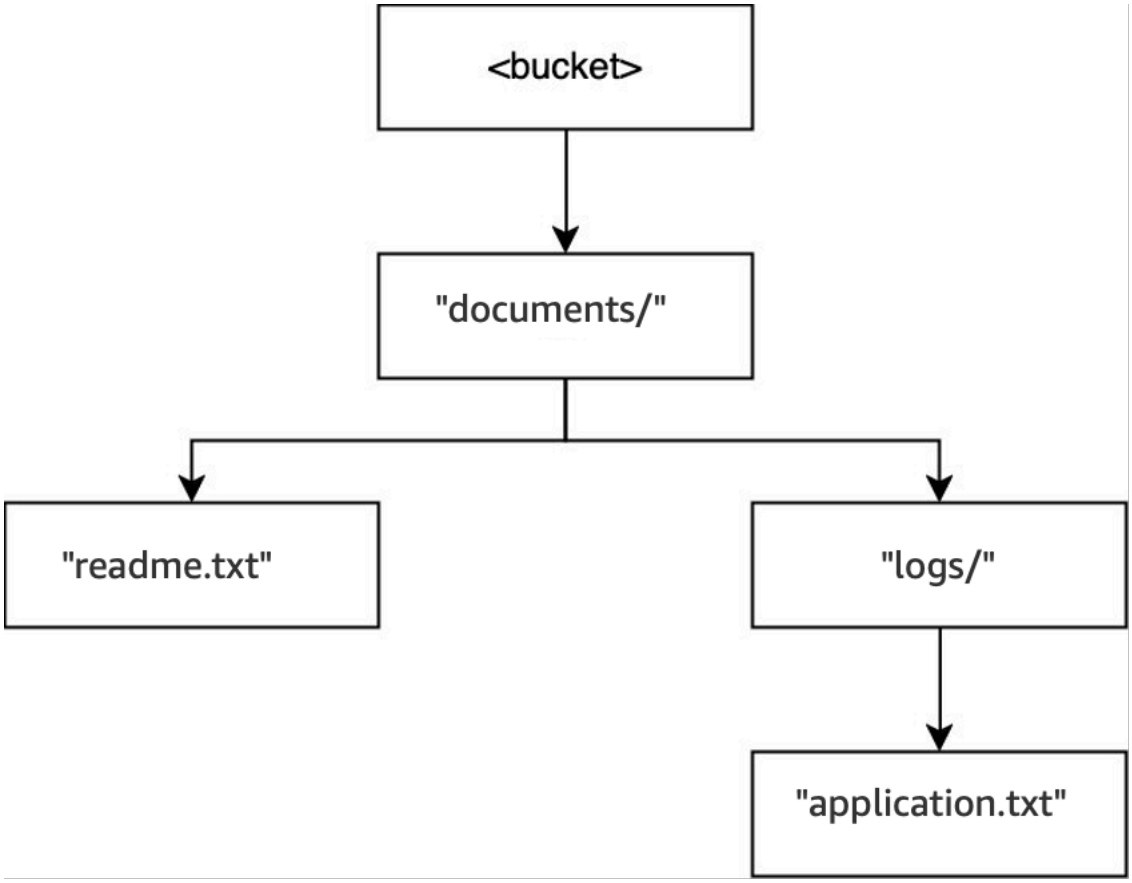
1. Lorsque a `LIST(<bucket>)` est exécuté, le répertoire `documents/` est saisi et la traversée commence.
2. Le sous-répertoire `logs/` est saisi et la traversée commence.
3. L'objet `application.txt` se trouve à l'intérieur`logs/`.
4. Aucune autre entrée n'existe dans`logs/`. L'opération List sort de `logs/` puis entre à `documents/` nouveau.
5. Le `documents/` répertoire continue d'être parcouru et l'objet `readme.txt` est trouvé.
6. Le `documents/` répertoire continue d'être parcouru, le sous-répertoire `reports/` est entré et le parcours commence.
7. L'objet `quarterly.txt` se trouve à l'intérieur`reports/`.
8. Aucune autre entrée n'existe dans`reports/`. La liste sort de la liste `reports/` et y entre `documents/` à nouveau.
9. Aucune autre entrée n'existe `documents/` et la liste revient.

Dans cet exemple, `logs/` est commandé avant `readme.txt` et `readme.txt` est commandé avant`reports/`.

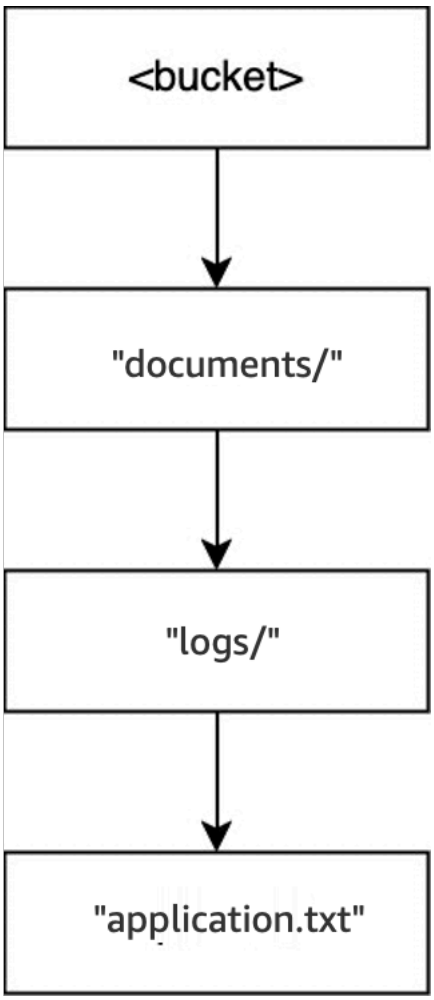
Exemple 3 : Comment les **`DeleteObject`** requêtes S3 adressées à un compartiment de répertoire interagissent avec les annuaires



1. Dans ce même compartiment, lorsque l'opération `DELETE(<bucket>, "documents/reports/quarterly.txt")` est exécutée, l'objet `quarterly.txt` est supprimé, laissant le répertoire `reports/` vide et provoquant sa suppression immédiate. Le `documents/` répertoire n'est pas vide car il contient à la fois le répertoire `logs/` et l'objet`readme.txt`. Il n'est donc pas supprimé. Pour cette opération, un seul objet et un seul répertoire ont été supprimés.



2. Lorsque l'opération `DELETE(<bucket>, "documents/readme.txt")` est exécutée, l'objet `readme.txt` est supprimé. `documents/`n'est toujours pas vide car il contient le répertoire`logs/`, il n'est donc pas supprimé. Pour cette opération, aucun répertoire n'est supprimé et seul l'objet est supprimé.



3. Enfin, lorsque l'opération `DELETE(<bucket>, "documents/logs/application.txt")` est exécutée, elle `application.txt` est supprimée, la laissant `logs/` vide et entraînant sa suppression immédiate. Cela reste alors `documents/` vide et le supprime également immédiatement. Pour cette opération, deux répertoires et un objet sont supprimés. Le compartiment est maintenant vide.



Charges de travail liées à la résidence des données

AWS Les zones locales dédiées (zones locales dédiées) sont un type d' AWS infrastructure entièrement géré par vous ou votre communauté AWS, conçu pour un usage exclusif par vous ou votre communauté, et placé dans un emplacement ou un centre de données que vous avez spécifié

pour vous aider à vous conformer aux exigences réglementaires. Les zones locales dédiées sont un type d'offre de zones AWS locales (zones locales). Pour plus d'informations, consultez Zones locales dédiées AWS.

Dans les Zones Locales dédiées, vous pouvez créer des compartiments d'annuaire S3 pour stocker les données dans un périmètre de données spécifique, ce qui permet de prendre en charge les cas d'utilisation liés à la résidence et à l'isolation des données. Les compartiments d'annuaire situés dans des zones locales dédiées peuvent prendre en charge les classes de stockage S3 Express One Zone et S3 One Zone-Infrequent Access (S3 One Zone-IA ; Z-IA). Les compartiments de répertoires ne sont actuellement pas disponibles dans les autres emplacements des zones locales AWS.

Vous pouvez utiliser l' AWS Management Console API REST AWS Command Line Interface (AWS CLI) et AWS SDKs dans des Zones Locales dédiées.

Pour plus d'informations sur l'utilisation des compartiments de répertoires dans les zones locales, consultez les rubriques suivantes :

Rubriques

- Concepts relatifs aux compartiments de répertoires dans les zones locales
- Activer les comptes pour les Zones Locales
- Connectivité privée depuis votre VPC
- Création d'un compartiment de répertoires dans une zone locale
- Authentification et autorisation des compartiments de répertoires dans les zones locales

Concepts relatifs aux compartiments de répertoires dans les zones locales

Avant de créer un bucket de répertoire dans une zone locale, vous devez disposer de l'ID de zone local dans lequel vous souhaitez créer un bucket. Vous pouvez trouver toutes les informations de la zone locale à l'aide de l'opération DescribeAvailabilityZonesAPI. Cette opération d'API répertorie des informations sur les zones locales, notamment leur zone locale IDs, les noms des régions parentes, les groupes de frontières du réseau et le statut d'inscription. Une fois que vous avez votre ID de zone locale et que vous êtes inscrit, vous pouvez créer un bucket de répertoire dans la zone locale. Un nom de compartiment de répertoire se compose d'un nom de base que vous fournissez et d'un suffixe contenant l'ID de zone de l'emplacement de votre compartiment, suivi `--x-s3` de.

Une zone locale est connectée à la région parent via le réseau privé redondant et à très haut débit Amazon. Cela donne aux applications exécutées dans la zone locale un accès rapide, sécurisé et

fluide au reste de la Services AWS région parent. L'ID de zone parent est l'ID de la zone qui gère les opérations du plan de contrôle de la zone locale. Network Border Group est un groupe unique à partir duquel sont AWS publiées des adresses IP publiques. Pour plus d'informations sur les zones locales, la région parente et l'ID de zone parent, consultez la section Concepts des zones AWS locales dans le Guide de l'utilisateur des zones AWS locales.

Tous les compartiments de répertoire utilisent l'espace de `s3express` noms, qui est distinct de l'espace de `s3` noms pour les compartiments à usage général. Pour les compartiments de répertoires, les demandes sont acheminées vers un point de terminaison régional ou un point de terminaison zonal. Le routage est géré automatiquement pour vous si vous utilisez le AWS Management Console AWS CLI, ou AWS SDKs.

La plupart des opérations d'API au niveau du bucket (telles que `CreateBucket` et`DeleteBucket`) sont acheminées vers des points de terminaison régionaux et sont appelées opérations d'API de point de terminaison régional. Les points de terminaison régionaux sont au format `s3express-control.ParentRegionCode.amazonaws.com`. Toutes les opérations d'API au niveau de l'objet (telles que `PutObject`) et deux opérations d'API au niveau du compartiment (`CreateSession` et `HeadBucket`) sont acheminées vers des points de terminaison zonaux et sont appelées opérations d'API de point de terminaison zonal. Les points de terminaison zonaux sont au format `s3express-LocalZoneID.ParentRegionCode.amazonaws.com`. Pour obtenir la liste complète des opérations d'API par type de point de terminaison, consultez Opérations d'API des compartiments de répertoires.

S3 est disponible dans la zone locale de Pékin :

ID de zone locale : `cnn1-pkx1-az1`

- Nom de la région parent : `China (Beijing)`
- Code de région parent : `cn-north-1`
- Zone réservée aux parents IDs : `cnn1-az1`
- Nom de la zone locale : `China (Beijing)`
- Code de zone local : `cnn1-pkx1-az1`
- Groupe frontalier du réseau : `cn-north-1-pkx-1`
- Exemple d'ARN de bucket : `arn:aws-cn:s3express:cn-north-1:`*`123456789012`*`:bucket/`*`amzn-s3-demo-bucket`*`--cnn1-pkx1-az1--x-s3`

Point de terminaison régional : `s3express-control.cn-north-1.amazonaws.com.cn`

Point de terminaison zonal : `s3express-cnn1-pkx1-az1.cn-north-1.amazonaws.com.cn`

Classe de stockage : `S3 One Zone-Infrequent Access (S3 One Zone-IA; Z-IA)`

Pour accéder aux compartiments de répertoires dans les zones locales à partir de votre cloud privé virtuel (VPC), vous pouvez utiliser des points de terminaison de VPC de passerelle. Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle. Pour configurer les points de terminaison de VPC de passerelle afin d'accéder aux compartiments de répertoires et aux objets dans les zones locales, consultez Connectivité privée depuis votre VPC.

Activer les comptes pour les Zones Locales

La rubrique suivante décrit comment les comptes sont activés pour les zones locales dédiées.

Pour tous les services des zones locales AWS dédiées (zones locales dédiées), y compris Amazon S3, votre administrateur doit les activer Compte AWS avant que vous puissiez créer une ressource dans la zone locale dédiée ou y accéder. Vous pouvez utiliser l'opération DescribeAvailabilityZonesAPI pour confirmer l'accès de votre identifiant de compte à une zone locale.

Pour mieux protéger vos données dans Amazon S3, par défaut, vous n'avez accès qu'aux ressources S3 que vous créez. Les compartiments dans les zones locales ont tous les paramètres de blocage de l'accès public S3 activés, et la propriété des objets S3 est défini sur Propriétaire du compartiment appliqué. Ces paramètres ne peuvent pas être modifiés. Vous pouvez utiliser la clé de condition `s3express:AllAccessRestrictedToLocalZoneGroup` dans vos politiques IAM pour que l'accès n'ait lieu qu'au sein des groupes de bordure réseau des zones locales. Pour de plus amples informations, veuillez consulter Authentification et autorisation des compartiments de répertoires dans les zones locales.

Connectivité privée depuis votre VPC

Vous pouvez utiliser un point de terminaison de passerelle pour accéder à des compartiments de répertoire AWS situés dans des zones locales (zones locales) depuis votre cloud privé virtuel (VPC), sans avoir besoin d'une passerelle Internet ou d'un périphérique NAT pour votre VPC, et sans frais supplémentaires. La rubrique suivante décrit la configuration des points de terminaison de VPC de passerelle entre votre VPC et les compartiments de répertoires dans les zones locales.

Pour configurer un point de terminaison de VPC de passerelle

1. Ouvrez la console Amazon VPC.
2. Dans le volet de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Créez un nom pour votre point de terminaison.
5. Pour Service category (Catégorie de service), choisissez Services AWS.
6. Pour les services, ajoutez le filtre Type=Gateway, puis cliquez sur le bouton d'option à côté de com.amazonaws. ***region***.s3 express.
7. Pour VPC, choisissez le VPC dans lequel créer le point de terminaison.
8. Pour Tables de routage, sélectionnez la table de routage de votre zone locale qui sera utilisée par le point de terminaison. Une fois le point de terminaison créé, un enregistrement de l'acheminement est ajouté à la table de routage que vous avez sélectionnée à cette étape.
9. Pour Politique, choisissez Accès complet afin d'autoriser toutes les opérations de tous les principaux sur toutes les ressources via le point de terminaison de VPC. Sinon, choisissez Personnalisé pour attacher une politique de point de terminaison de VPC qui contrôle les autorisations dont disposent les principaux pour effectuer des actions au niveau des ressources via le point de terminaison de VPC.
10. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
11. Choisissez Créer un point de terminaison.

Pour en savoir plus sur les points de terminaison d'un VPC de passerelle, consultez Points de terminaison de VPC de passerelle dans le Guide AWS PrivateLink . Pour les cas d'utilisation de la résidence des données, nous vous recommandons de n'autoriser l'accès à vos compartiments qu'à partir de votre VPC à l'aide de points de terminaison de VPC de passerelle. Lorsque l'accès est limité à un VPC ou à un point de terminaison VPC, vous pouvez accéder aux objets via l' AWS Management Console API REST et. AWS CLI AWS SDKs

> **Note**
>
> Pour restreindre l'accès à un VPC ou à un point de terminaison VPC à l'aide du AWS Management Console, vous devez utiliser l'accès privé. AWS Management Console Pour

plus d'informations, consultez Accès privé de la AWS Management Console dans le Guide de l'utilisateur de la AWS Management Console .

Création d'un compartiment de répertoires dans une zone locale

Dans les zones locales dédiées, vous pouvez créer des compartiments de répertoires pour stocker et récupérer des objets dans un périmètre de données spécifique afin de répondre à vos cas d'utilisation liés à la résidence et à l'isolement des données. Les compartiments de répertoires S3 sont le seul type de compartiment pris en charge dans les zones locales et contiennent un type d'emplacement de compartiment appelé `LocalZone`. Le nom d'un compartiment de répertoires se compose d'un nom de base que vous fournissez et d'un suffixe contenant l'ID de la zone dans laquelle se trouve votre compartiment, et `--x-s3`. Vous pouvez obtenir une liste des zones locales à IDs l'aide de l'opération DescribeAvailabilityZonesAPI. Pour de plus amples informations, veuillez consulter Règles de dénomination des compartiments de répertoires.

> **Note**
>
> - Pour tous les services des zones locales AWS dédiées (zones locales dédiées), y compris S3, votre administrateur doit les activer Compte AWS avant que vous puissiez créer une ressource dans la zone locale dédiée ou y accéder. Pour de plus amples informations, veuillez consulter Activer les comptes pour les Zones Locales.
> - Pour les exigences relatives à la résidence des données, nous vous recommandons de n'autoriser l'accès à vos compartiments qu'à partir des points de terminaison de VPC de passerelle. Pour de plus amples informations, veuillez consulter Connectivité privée depuis votre VPC.
> - Vous pouvez aussi utiliser la clé de condition `s3express:AllAccessRestrictedToLocalZoneGroup` dans vos politiques IAM pour que l'accès n'ait lieu qu'au sein des groupes de bordure réseau des zones locales. Pour de plus amples informations, veuillez consulter Authentification et autorisation des compartiments de répertoires dans les zones locales.

Ce qui suit décrit les méthodes de création d'un bucket de répertoire dans une seule zone locale avec le AWS Management Console AWS CLI, et AWS SDKs.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région parent d'une zone locale dans laquelle vous souhaitez créer un compartiment de répertoires.

   > **Note**
   >
   > Pour plus d'informations sur les régions parents, consultez Concepts relatifs aux compartiments de répertoires dans les zones locales.

3. Dans le panneau de navigation de gauche, choisissez Compartiments.
4. Choisissez Créer un compartiment.

   La page Créer un compartiment s'ouvre.
5. Sous Configuration générale, consultez la Région AWS dans laquelle votre compartiment sera créé.
6. Sous Type de compartiment, choisissez Répertoire.

   > **Note**
   >
   > - Si vous avez choisi une région qui ne prend pas en charge les compartiments de répertoires, le type de compartiment est défini par défaut sur un compartiment à usage général. Pour créer un compartiment de répertoires, vous devez choisir une région prise en charge. Pour obtenir la liste des régions prises en charge par les compartiments de répertoires, consultez the section called "Points de terminaison d'API régionaux et zonaux des compartiments de répertoires".
   > - Une fois que vous avez créé le compartiment, vous ne pouvez pas modifier son type.

7. Sous Emplacement du compartiment, choisissez la zone locale que vous souhaitez utiliser.

   > **Note**
   >
   > La zone locale ne peut pas être modifiée une fois le compartiment créé.

8. Sous Emplacement du compartiment, cochez la case pour reconnaître qu'en cas de panne de la zone locale, vos données pourraient être indisponibles ou perdues.

   > **Important**
   >
   > Les compartiments de répertoires sont stockés sur plusieurs appareils au sein d'une même zone locale, mais ne stockent pas les données de manière redondante entre les zones locales.

9. Pour Nom du compartiment, entrez un nom pour votre compartiment de répertoires.

   Pour plus d'informations sur les règles de dénomination des compartiments de répertoires, consultez Règles de dénomination des compartiments à usage général. Un suffixe est automatiquement ajouté au nom de base que vous fournissez lorsque vous créez un compartiment de répertoires à l'aide de la console. Ce suffixe inclut l'ID de la zone locale que vous avez choisie.

   Une fois le compartiment créé, vous ne pouvez pas changer son nom.

   > **Important**
   >
   > N'ajoutez pas d'informations sensibles, notamment des numéros de compte, dans le nom du compartiment. Le nom du bucket est visible URLs là où pointent les objets du bucket.

10. Sous Propriété de l'objet, le paramètre imposé au propriétaire du compartiment est automatiquement activé et toutes les listes de contrôle d'accès (ACLs) sont désactivées. Pour les compartiments de répertoire, ACLs ils sont désactivés et ne peuvent pas être activés.

    Lorsque le paramètre « propriétaire du compartiment forcé » est activé, le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. ACLs n'affecte plus les autorisations d'accès aux données du compartiment S3. Le compartiment utilise des stratégies exclusivement pour définir le contrôle des accès. La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

11. Sous Paramètres de blocage de l'accès public pour ce compartiment, notez que les paramètres de blocage de l'accès public pour votre compartiment de répertoires sont automatiquement

activés. Ces paramètres ne peuvent pas être modifiés pour les compartiments de répertoires. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

12. Dans Chiffrement par défaut, les compartiments de répertoires utilisent le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) pour chiffrer les données par défaut. Vous avez également la possibilité de chiffrer les données dans des compartiments d'annuaire grâce au chiffrement côté serveur à l'aide de AWS Key Management Service clés (SSE-KMS).
13. Choisissez Créer un compartiment.

    Après avoir créé le compartiment, vous pouvez y ajouter des fichiers et des dossiers. Pour de plus amples informations, veuillez consulter the section called "Utilisation d'objets dans un compartiment de répertoires".

À l'aide du AWS CLI

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez-la *user input placeholders* par vos propres informations.

Lorsque vous créez un compartiment de répertoires, vous devez fournir les détails de configuration et utiliser la convention de dénomination suivante : *bucket-base-name*--*zone-id*--x-s3.

```
aws s3api create-bucket
--bucket bucket-base-name--zone-id--x-s3
--create-bucket-configuration 'Location={Type=LocalZone,Name=local-zone-
id},Bucket={DataRedundancy=SingleLocalZone,Type=Directory}'
--region parent-region-code
```

Pour plus d'informations sur l'ID de zone locale et le code de la région parent, consultez Concepts relatifs aux compartiments de répertoires dans les zones locales. Pour plus d'informations sur la commande AWS CLI , consultez create-bucket dans la Référence des commandes de l'AWS CLI .

À l'aide du AWS SDKs

SDK for Go

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' AWS SDK pour Go.

Example

```
var bucket = "bucket-base-name--zone-id--x-s3" // The full directory bucket name

func runCreateBucket(c *s3.Client) {
    resp, err := c.CreateBucket(context.Background(), &s3.CreateBucketInput{
        Bucket: &bucket,
        CreateBucketConfiguration: &types.CreateBucketConfiguration{
            Location: &types.LocationInfo{
                Name: aws.String("local-zone-id"),
                Type: types.LocationTypeLocalZone,
            },
            Bucket: &types.BucketInfo{
                DataRedundancy: types.DataRedundancySingleLocalZone,
                Type:           types.BucketTypeDirectory,
            },
        },
    })
    var terr *types.BucketAlreadyOwnedByYou
    if errors.As(err, &terr) {
        fmt.Printf("BucketAlreadyOwnedByYou: %s\n", aws.ToString(terr.Message))
        fmt.Printf("noop...\n") // No operation performed, just printing a message
        return
    }
    if err != nil {
        log.Fatal(err)
    }

    fmt.Printf("bucket created at %s\n", aws.ToString(resp.Location))
}
```

SDK for Java 2.x

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' AWS SDK for Java 2.x.

Example

```
public static void createBucket(S3Client s3Client, String bucketName) {

    //Bucket name format is {base-bucket-name}--{local-zone-id}--x-s3
    //example: doc-example-bucket--local-zone-id--x-s3 is a valid name for a
 directory bucket created in a Local Zone.
```

```
   CreateBucketConfiguration bucketConfiguration =
CreateBucketConfiguration.builder()
            .location(LocationInfo.builder()
                    .type(LocationType.LOCAL_ZONE)
                    .name("local-zone-id").build()) //this must match the Local
Zone ID in your bucket name
            .bucket(BucketInfo.builder()
                   .type(BucketType.DIRECTORY)
                   .dataRedundancy(DataRedundancy.SINGLE_LOCAL_ZONE)
                   .build()).build();
   try {

            CreateBucketRequest bucketRequest =
CreateBucketRequest.builder().bucket(bucketName).createBucketConfiguration(bucketConfigurat
            CreateBucketResponse response = s3Client.createBucket(bucketRequest);
            System.out.println(response);
   }

   catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
        }
   }
```

AWS SDK pour JavaScript

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' AWS SDK pour JavaScript.

Example

```
// file.mjs, run with Node.js v16 or higher
// To use with the preview build, place this in a folder
// inside the preview build directory, such as /aws-sdk-js-v3/workspace/

import { S3 } from "@aws-sdk/client-s3";

const region = "parent-region-code";
const zone = "local-zone-id";
const suffix = `${zone}--x-s3`;
```

```
const s3 = new S3({ region });

const bucketName = `bucket-base-name--${suffix}`; // Full directory bucket name

const createResponse = await s3.createBucket(
    { Bucket: bucketName,
      CreateBucketConfiguration: {Location: {Type: "LocalZone", Name: "local-zone-
id"},
      Bucket: { Type: "Directory", DataRedundancy: "SingleLocalZone" }}
    }
   );
```

SDK pour .NET

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' SDK pour .NET.

Example

```
using (var amazonS3Client = new AmazonS3Client())
{
    var putBucketResponse = await amazonS3Client.PutBucketAsync(new PutBucketRequest
    {

       BucketName = "bucket-base-name--local-zone-id--x-s3",
       PutBucketConfiguration = new PutBucketConfiguration
       {
         BucketInfo = new BucketInfo { DataRedundancy =
 DataRedundancy.SingleLocalZone, Type = BucketType.Directory },
         Location = new LocationInfo { Name = "local-zone-id", Type =
 LocationType.LocalZone }
       }
     }).ConfigureAwait(false);
}
```

SDK for PHP

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' AWS SDK for PHP.

Example

```
require 'vendor/autoload.php';
```

```
$s3Client = new S3Client([

    'region'      => 'parent-region-code',
]);


$result = $s3Client->createBucket([
    'Bucket' => 'bucket-base-name--local-zone-id--x-s3',
    'CreateBucketConfiguration' => [
        'Location' => ['Name'=> 'local-zone-id', 'Type'=> 'LocalZone'],
        'Bucket' => ["DataRedundancy" => "SingleLocalZone" ,"Type" => "Directory"]
  ],
]);
```

SDK for Python

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' AWS SDK pour Python (Boto3).

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def create_bucket(s3_client, bucket_name, local_zone):
    '''
    Create a directory bucket in a specified Local Zone

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to create; for example, 'bucket-base-name--local-
zone-id--x-s3'
    :param local_zone: String; Local Zone ID to create the bucket in
    :return: True if bucket is created, else False
    '''

    try:
        bucket_config = {
                'Location': {
                    'Type': 'LocalZone',
                    'Name': local_zone
                },
                'Bucket': {
                    'Type': 'Directory',
```

```
                    'DataRedundancy': 'SingleLocalZone'
                }
            }
        s3_client.create_bucket(
            Bucket = bucket_name,
            CreateBucketConfiguration = bucket_config
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'parent-region-code'
    local_zone = 'local-zone-id'
    s3_client = boto3.client('s3', region_name = region)
    create_bucket(s3_client, bucket_name, local_zone)
```

SDK for Ruby

Cet exemple montre comment créer un compartiment de répertoires dans une zone locale à l'aide du kit AWS SDK pour Ruby.

Example

```
s3 = Aws::S3::Client.new(region:'parent-region-code')
s3.create_bucket(
  bucket: "bucket-base-name--local-zone-id--x-s3",
  create_bucket_configuration: {
    location: { name: 'local-zone-id', type: 'LocalZone' },
    bucket: { data_redundancy: 'SingleLocalZone', type: 'Directory' }
  }
)
```

Authentification et autorisation des compartiments de répertoires dans les zones locales

Les compartiments d'annuaire des Zones Locales prennent en charge à la fois l'autorisation AWS Identity and Access Management (IAM) et l'autorisation basée sur les sessions. Pour plus

d'informations sur l'authentification et l'autorisation des compartiments de répertoires, consultez Authentification et autorisation des demandes.

Ressources

Amazon Resource Names (ARNs) pour les compartiments de répertoire contient l'`s3express`espace de noms, la région AWS parent, l' Compte AWS ID et le nom du compartiment de répertoire qui inclut l'ID de zone. Pour accéder à votre compartiment de répertoires et y effectuer des actions, vous devez utiliser le format d'ARN suivant :

```
arn:aws:s3express:region-code:account-id:bucket/bucket-base-name--ZoneID--x-s3
```

Pour les compartiments de répertoires d'une zone locale, l'ID de zone est l'ID de la zone locale. Pour plus d'informations sur les compartiments de répertoires dans les zones locales, consultez Concepts relatifs aux compartiments de répertoires dans les zones locales. Pour plus d'informations ARNs, consultez Amazon Resource Names (ARNs) dans le guide de l'utilisateur IAM. Pour plus d'informations sur les ressources, consultez Éléments de politique JSON IAM : Resource dans le Guide de l'utilisateur IAM.

Clés de condition des compartiments de répertoires dans les zones locales

Dans les Zones Locales, vous pouvez utiliser toutes ces clés de condition dans vos politiques IAM. En outre, pour créer un périmètre de données autour des groupes de bordure réseau de votre zone locale, vous pouvez utiliser la clé de condition `s3express:AllAccessRestrictedToLocalZoneGroup` afin de refuser toutes les demandes provenant d'en dehors de ces groupes.

La clé de condition suivante peut être utilisée pour affiner les conditions d'application d'une déclaration de politique IAM. Pour obtenir la liste complète des opérations d'API, des actions de politique et des clés de condition prises en charge par les compartiments de répertoires, consultez Actions de politique pour les compartiments de répertoires.

> **Note**
>
> La clé de condition suivante s'applique uniquement aux zones locales et n'est pas prise en charge dans les zones de disponibilité ni dans les Régions AWS.

Opérations d'API	Actions de politique	Description	Clé de condition	Description	Type
Opérations d'API de point de terminaison zonal	s3express:CreateSession	Accorde l'autorisation de créer un jeton de session, qui est utilisé pour accorder l'accès à toutes les opérations d'API de point de terminaison zonal, telles que CreateSession , HeadBucket , CopyObject , PutObject et GetObject .	s3express:AllAccessRestrictedToLocalZoneGroup	Filtre tous les accès au bucket, sauf si la demande provient des groupes frontaliers du réseau de zones AWS locales fournis dans cette clé de condition. Valeurs : valeur du groupe de bordure réseau des zones locales	String

Exemples de politiques

Pour restreindre l'accès aux objets aux demandes provenant d'une limite de résidence des données que vous définissez (en particulier, un groupe de zones locales qui est un ensemble de zones locales apparentées à la même Région AWS), vous pouvez définir l'une des politiques suivantes :

- Politique de contrôle des services (SCP). Pour plus d'informations SCPs, voir Politiques de contrôle des services (SCPs) dans le Guide de AWS Organizations l'utilisateur.
- Politique basée sur l'identité IAM pour le rôle IAM.
- Politique de point de terminaison d'un VPC. Pour obtenir des informations sur les politiques de point de terminaison d'un VPC, consultez Contrôle de l'accès aux points de terminaison d'un VPC à l'aide de politiques de point de terminaison dans le Guide AWS PrivateLink .
- Politique de compartiment S3.

> **Note**
>
> La clé de condition `s3express:AllAccessRestrictedToLocalZoneGroup` ne prend pas en charge l'accès depuis un environnement sur site. Pour prendre en charge l'accès

depuis un environnement sur site, vous devez ajouter l'adresse IP source aux politiques. Pour plus d'informations, consultez aws : SourceIp dans le guide de l'utilisateur IAM.

Example — Politique SCP

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Effect": "Deny",
            "Action": [
                "s3express:*",
            ],
            "Resource": "*",
            "Condition": {
                "StringNotEqualsIfExists": {
                    "s3express:AllAccessRestrictedToLocalZoneGroup": [
                        "local-zone-network-border-group-value"
                    ]
                }
            }
        }
    ]
}
```

Example — Politique basée sur l'identité IAM (attachée au rôle IAM)

JSON

```
{
    "Version": "2012-10-17",
    "Statement": {
        "Effect": "Deny",
        "Action": "s3express:CreateSession",
        "Resource": "*",
        "Condition": {
```

```
            "StringNotEqualsIfExists": {
                "s3express:AllAccessRestrictedToLocalZoneGroup": [
                    "local-zone-network-border-group-value"
                ]
            }
        }
    }
}
```

Example – politique de point de terminaison de VPC

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                 "StringNotEqualsIfExists": {
                     "s3express:AllAccessRestrictedToLocalZoneGroup": [
                         "local-zone-network-border-group-value"
                     ]
                 }
            }
        }
    ]
}
```

Example – politique de compartiment

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Access-to-specific-LocalZones-only",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                 "StringNotEqualsIfExists": {
                     "s3express:AllAccessRestrictedToLocalZoneGroup": [
                         "local-zone-network-border-group-value"
                     ]
                 }
            }
        }
    ]
}
```

Différences pour les compartiments de répertoires

Lorsque vous utilisez Amazon S3, vous pouvez choisir le type de compartiment qui correspond le mieux à votre application et à vos exigences de performances. Un bucket d'annuaire est un type de bucket idéal pour les cas d'utilisation à faible latence ou en cas de résidence de données. Pour en savoir plus sur les compartiments de répertoire, consultezUtilisation des compartiments de répertoires.

Pour plus d'informations sur les différences entre les compartiments de répertoires, consultez les rubriques suivantes.

Rubriques

- Différences pour les compartiments de répertoires

- Opérations d'API prises en charge pour les compartiments de répertoires
- Fonctionnalités Amazon S3 non prises en charge par les compartiments de répertoires

Différences pour les compartiments de répertoires

- Noms des compartiments de répertoires
  - Le nom d'un bucket d'annuaire se compose d'un nom de base que vous fournissez et d'un suffixe contenant l'ID de la AWS zone (zone de disponibilité ou zone locale) dans laquelle se trouve votre bucket, suivi `--x-s` de. Pour obtenir une liste de règles et des exemples de noms de compartiments de répertoires, consultez Règles de dénomination des compartiments de répertoires.
- Comportement de **`ListObjectsV2`**
  - Pour les compartiments de répertoires, `ListObjectsV2` ne renvoie pas les objets par ordre lexicographique (alphabétique). De plus, les préfixes doivent se terminer par un délimiteur et seul « / » peut être spécifié comme délimiteur.
  - Pour les compartiments de répertoires, la réponse `ListObjectsV2` inclut les préfixes liés uniquement aux chargements partitionnés en cours.
- Comportement de suppression : lorsque vous supprimez un objet dans un compartiment de répertoires, Amazon S3 supprime de manière récursive tous les répertoires vides au niveau du chemin de l'objet. Par exemple, si vous supprimez la clé d'objet `dir1/dir2/file1.txt`, Amazon S3 supprime `file1.txt`. Si les répertoires `dir1/` et `dir2/` sont vides et ne contiennent aucun autre objet, Amazon S3 supprime également ces répertoires.
- ETags et sommes de contrôle — Les balises d'entité (ETags) pour les compartiments de répertoire sont des chaînes alphanumériques aléatoires propres à l'objet et non des sommes de contrôle. MD5 Pour plus d'informations sur l'utilisation de sommes de contrôle supplémentaires avec des compartiments de répertoire, consultez. Bonnes pratiques supplémentaires en matière de somme de contrôle S3
- Clés d'objet dans les demandes **`DeleteObjects`**
  - Les clés d'objet figurant dans les demandes `DeleteObjects` doivent contenir au moins un caractère autre qu'une espace. Les chaînes composées uniquement de caractères espace ne sont pas prises en charge dans les demandes `DeleteObjects`.
  - Les clés d'objet figurant dans les demandes `DeleteObjects` ne peuvent pas contenir de caractères de contrôle Unicode, à l'exception des caractères de saut de ligne (`\n`), de tabulation (`\t`) et de retour chariot (`\r`).

- Points de terminaison régionaux et zonaux : les opérations d'API de gestion des compartiments de répertoires sont disponibles via un point de terminaison régional et sont appelées API de point de terminaison régional. Des exemples d'opérations d'API de point de terminaison régional sont CreateBucket et DeleteBucket. Après avoir créé un compartiment de répertoires, vous pouvez utiliser les opérations d'API de point de terminaison zonal pour charger et gérer les objets dans votre compartiment de répertoires. Les opérations d'API de point de terminaison zonal sont disponibles via un point de terminaison zonal. `PutObject` et `CopyObject` sont des exemples d'opérations d'API de point de terminaison zonal. Lorsque vous utilisez des compartiments de répertoires, vous devez spécifier la région dans toutes les demandes. Pour les points de terminaison régionaux, vous spécifiez la région, par exemple `s3express-control.us-west-2.amazonaws.com`. Pour les points de terminaison zonaux, vous spécifiez à la fois la région et la zone de disponibilité, par exemple `s3express-usw2-az1.us-west-2.amazonaws.com`. Pour de plus amples informations, veuillez consulter Points de terminaison d'API régionaux et zonaux des compartiments de répertoires.
- Chargements partitionnés : vous pouvez charger et copier les objets volumineux stockés dans des compartiments de répertoires à l'aide du processus de chargement partitionné. Toutefois, voici quelques différences qui s'appliquent lors de l'utilisation du processus de chargement partitionné avec des objets stockés dans des compartiments de répertoires. Pour de plus amples informations, veuillez consulter the section called "Utilisation du chargement partitionné avec les compartiments de répertoires".
  - La date de création de l'objet correspond à la date d'achèvement du chargement partitionné.
  - Les numéros de parties partitionnés doivent utiliser des numéros de parties consécutifs. Si vous essayez d'effectuer une demande de chargement partitionné avec des numéros de parties non consécutifs, Amazon S3 génère une erreur HTTP `400 (Bad Request)`.
  - L'initiateur d'un chargement partitionné ne peut abandonner la demande de chargement partitionné que s'il a obtenu une autorisation d'accès explicite à `AbortMultipartUpload` via l'autorisation `s3express:CreateSession`. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM.
- Videz un compartiment de répertoire : la `s3 rm` commande via la AWS Command Line Interface (CLI), l'`delete`opération via Mountpoint et le bouton d'option Empty bucket via le ne permettent pas de supprimer les téléchargements AWS Management Console partitionnés en cours dans un compartiment de répertoire. Pour supprimer ces chargements partitionnés en cours, utilisez l'opération `ListMultipartUploads` afin d'afficher les chargements partitionnés en cours dans le compartiment et utilisez l'opération `AbortMultipartUpload` pour abandonner tous les chargements partitionnés en cours.

- AWS Zones locales : les zones locales ne sont prises en charge que pour les compartiments de répertoire et non pour les compartiments à usage général.
  - L'ajout de données à des objets existants n'est pas pris en charge pour les compartiments de répertoire situés dans des Zones Locales. Vous pouvez uniquement ajouter des données à des objets existants dans des compartiments de répertoire situés dans des zones de disponibilité.
  - S3 Lifecycle n'est pas pris en charge pour les compartiments de répertoire dans les Zones Locales.

Opérations d'API prises en charge pour les compartiments de répertoires

Les compartiments d'annuaire prennent en charge les opérations d'API de point de terminaison régionales (niveau du compartiment ou plan de contrôle) et zonales (niveau objet ou plan de données). Pour plus d'informations, consultez Mise en réseau des compartiments de répertoires et Points de terminaison et points de terminaison de VPC de passerelle. Pour obtenir la liste des opérations d'API prises en charge, voirOpérations d'API des compartiments de répertoires.

Fonctionnalités Amazon S3 non prises en charge par les compartiments de répertoires

Les fonctionnalités Amazon S3 suivantes ne sont pas prises en charge par les compartiments d'annuaire :

- AWS politiques gérées
- AWS PrivateLink pour S3
- MD5 sommes de contrôle
- Suppression de l'authentification multifacteur (MFA)
- Verrouillage des objets S3
- paiement par le demandeur
- Autorisations d'accès S3
- Métriques relatives aux CloudWatch demandes Amazon
- Notifications d'événements S3
- Actions de transition du cycle de vie S3
- Points d'accès multirégionaux S3
- Points d'accès S3 Object Lambda

- Gestion des versions S3
- Inventaire S3
- Réplication S3
- Balises d'objet
- S3 Select
- Journaux d'accès de serveur
- Hébergement de site Web statique
- S3 Storage Lens
- Groupes S3 Storage Lens
- S3 Transfer Acceleration
- Chiffrement double couche côté serveur avec clés AWS Key Management Service (AWS KMS) (DSSE-KMS)
- Chiffrement côté serveur avec clés fournies par le client (SSE-C)
- Option permettant de copier les paramètres d'un compartiment existant lors de la création d'un compartiment dans la console Amazon S3
- Messages d'erreur de refus d'accès améliorés (HTTP `403 Forbidden`)

Mise en réseau des compartiments de répertoires

Pour accéder aux compartiments de répertoires et aux objets qu'ils contiennent, vous utilisez des points de terminaison d'API régionaux et zonaux différents des points de terminaison Amazon S3 standard. Selon l'opération d'API S3 que vous utilisez, un point de terminaison zonal ou régional est requis. Pour obtenir la liste complète des opérations d'API par type de point de terminaison, consultez Différences pour les compartiments de répertoires.

Vous pouvez accéder aux opérations d'API zonales et régionales via des points de terminaison de cloud privé virtuel (VPC) de passerelle.

Les rubriques suivantes décrivent les exigences de mise en réseau pour accéder à S3 Express One Zone à l'aide d'un point de terminaison de VPC de passerelle.

Rubriques

- Points de terminaison

- Configuration de points de terminaison de VPC de passerelle

Points de terminaison

Vous pouvez accéder aux compartiments de répertoires et à leurs objets à partir de votre VPC en utilisant des points de terminaison de VPC de passerelle. Les compartiments de répertoires utilisent des points de terminaison d'API régionaux et zonaux. Selon l'opération d'API Amazon S3 que vous utilisez, un point de terminaison régional ou zonal est requis. Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle.

Les opérations d'API de niveau compartiment (ou plan de contrôle) sont disponibles via les points de terminaison régionaux et sont appelées opérations d'API de point de terminaison régional. `CreateBucket` et `DeleteBucket` sont des exemples d'opérations d'API de point de terminaison régional. Lorsque vous créez un compartiment de répertoires, vous choisissez une zone (zone de disponibilité ou zone locale) dans laquelle ce compartiment sera créé. Après avoir créé un compartiment de répertoires, vous pouvez utiliser les opérations d'API de point de terminaison zonal pour charger et gérer les objets dans votre compartiment de répertoires.

Les opérations d'API de niveau objet (ou plan de données) sont disponibles via les points de terminaison zonaux et sont appelées opérations d'API de point de terminaison zonal. `CreateSession` et `PutObject` sont des exemples d'opérations d'API de point de terminaison zonal.

Pour plus d'informations sur les points de terminaison et les emplacements qui prennent en charge les compartiments de répertoires dans les zones de disponibilité, consultez Points de terminaison des compartiments de répertoires situés dans des zones de disponibilité.

Pour plus d'informations sur les points de terminaison et les emplacements qui prennent en charge les compartiments de répertoires dans les zones locales, consultez Activer les comptes pour les Zones Locales.

Configuration de points de terminaison de VPC de passerelle

Pour configurer des points de terminaison de VPC de passerelle pour l'accès aux compartiments de répertoires dans les zones de disponibilité, consultez the section called "Configuration de points de terminaison de VPC de passerelle".

Pour configurer des points de terminaison de VPC de passerelle pour l'accès aux compartiments de répertoires dans les zones locales, consultez Connectivité privée depuis votre VPC.

Règles de dénomination des compartiments de répertoires

Lorsque vous créez un compartiment de répertoires dans Amazon S3, les règles de dénomination suivantes s'appliquent. Pour connaître les règles de dénomination des compartiments à usage général, consultez Règles de dénomination des compartiments à usage général.

Le nom d'un bucket d'annuaire se compose d'un nom de base que vous fournissez et d'un suffixe contenant l'ID de la AWS zone (une zone de disponibilité ou une zone locale) dans laquelle se trouve votre bucket. `--x-s3` Il *`zone-id`* peut s'agir de l'ID d'une zone de disponibilité ou d'une zone locale.

```
base-name--zoneid--x-s3
```

Par exemple, le nom de compartiment de répertoires suivant contient l'ID de zone de disponibilité `usw2-az1` :

```
bucket-base-name--usw2-az1--x-s3
```

> **Note**
>
> Lorsque vous créez un compartiment de répertoires à l'aide de la console, un suffixe est automatiquement ajouté au nom de base que vous fournissez. Ce suffixe inclut l'ID de la zone de disponibilité ou de la zone locale que vous avez choisie.
> Lorsque vous créez un compartiment de répertoires à l'aide d'une API, vous devez fournir le suffixe complet, y compris l'ID de zone, dans votre demande. Pour une liste des zones IDs, voirPoints de terminaison.

Les règles suivantes s'appliquent pour nommer les compartiments de répertoires :

- Soyez unique au sein de la zone choisie (zone de AWS disponibilité ou zone AWS locale).
- Le nom doit contenir entre 3 (minimum) et 63 caractères (maximum), suffixe inclus.
- Doit être composé uniquement de lettres minuscules, de chiffres et de traits d'union (-).
- Il doit commencer et se terminer par une lettre ou un chiffre.
- Doit inclure le suffixe suivant : `--`*`zone-id`*`--x-s3`
- Les noms de compartiment ne doivent pas commencer par le préfixe `xn--`.
- Les noms de compartiment ne doivent pas commencer par le préfixe `sthree-`.

- Les noms de compartiment ne doivent pas commencer par le préfixe `sthree-configurator`.
- Les noms de compartiment ne doivent pas commencer par le préfixe `amzn-s3-demo-`.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `-s3alias`. Ce suffixe est réservé aux noms d'alias de point d'accès. Pour plus d'informations, consultez Alias de point d'accès.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `--ol-s3`. Ce suffixe est réservé aux noms d'alias de point d'accès Object Lambda. Pour de plus amples informations, veuillez consulter Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda de compartiment S3.
- Les noms de compartiment ne doivent pas se terminer par le suffixe `.mrap`. Ce suffixe est réservé aux noms de point d'accès multi-régions. Pour de plus amples informations, veuillez consulter Règles relatives à l'attribution de noms pour les points d'accès multi-Régions Amazon S3.

Affichage des propriétés d'un compartiment de répertoires

Vous pouvez afficher et configurer les propriétés d'un compartiment de répertoires Amazon S3 à l'aide de la console S3. Pour de plus amples informations, veuillez consulter Utilisation des compartiments de répertoires.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Directory buckets.
3. Dans la liste Compartiments de répertoires, choisissez le nom du compartiment dont vous souhaitez afficher les propriétés.
4. Choisissez l'onglet Propriétés.
5. Sur la page Propriétés, vous pouvez consulter les propriétés suivantes pour le compartiment.

    - Vue d'ensemble du compartiment de répertoires : vous pouvez voir la Région AWS zone (zone de disponibilité ou zone locale), l'Amazon Resource Name (ARN) et la date de création du compartiment.
    - Paramètres de chiffrement côté serveur : Amazon S3 applique le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) comme niveau de base de chiffrement pour tous les compartiments S3. Amazon S3 chiffre un objet avant de l'enregistrer sur un disque

et déchiffre l'objet quand vous le téléchargez. Pour de plus amples informations, veuillez consulter Configuration et surveillance du chiffrement par défaut pour les compartiments de répertoires.

Pour plus d'informations sur les fonctionnalités prises en charge pour les compartiments de répertoires, consultez Création et utilisation de compartiments de répertoires.

Gestion des politiques des compartiments de répertoires

Vous pouvez ajouter, supprimer, mettre à jour et consulter les politiques de compartiment pour les compartiments d'annuaire Amazon S3 à l'aide de la console Amazon S3, de la CLI AWS SDKs et de la AWS CLI. Pour plus d'informations, consultez les rubriques suivantes. Pour plus d'informations sur les actions prises en charge AWS Identity and Access Management (IAM), consultezAutorisation des opérations d'API de point de terminaison régional avec IAM. Pour voir des exemples de politiques de compartiment pour les compartiments de répertoires, consultez Exemples de politiques de compartiment pour les compartiments de répertoires.

Rubriques

- Ajout d'une politique de compartiment
- Affichage d'une politique de compartiment
- Suppression d'une politique de compartiment

Ajout d'une politique de compartiment

Pour ajouter une politique de compartiment à un compartiment de répertoire, vous pouvez utiliser la console Amazon S3, le AWS SDKs, ou le AWS CLI.

Utilisation de la console S3

Pour créer ou modifier une politique de compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Directory buckets.
3. Dans la liste des compartiments du répertoire, choisissez le nom du compartiment auquel vous souhaitez ajouter une politique.

4. Sélectionnez l'onglet Autorisations.
5. Sous Politique de compartiment, choisissez Modifier. La page Edit bucket policy (Modifier la politique de compartiment) s'affiche.
6. Pour générer une politique automatiquement, choisissez Générateur de stratégies.

   Si vous choisissez le générateur de AWS politiques, celui-ci s'ouvre dans une nouvelle fenêtre.

   Si vous ne souhaitez pas utiliser le générateur de AWS politiques, vous pouvez ajouter ou modifier des instructions JSON dans la section Politique.

   a. Sur la page AWS Policy Generator (Générateur de politiques), pour Select Type of Policy (Sélectionner le type de politique), sélectionnez S3 Bucket Policy (Politique de compartiment S3).
   b. Ajoutez une instruction en saisissant les informations dans les champs fournis, puis choisissez Add Statement (Ajouter une instruction). Répétez l'opération pour autant d'instructions que vous souhaitez ajouter. Pour plus d'informations sur ces champs, consultez la Référence des éléments de politique IAM JSON dans le Guide de l'utilisateur IAM.

      > **Note**
      >
      > Pour plus de commodité, la page Modifier la stratégie de compartiment affiche l'ARN (Amazon Resource Name) du compartiment actuel au-dessus du champ de texte Stratégie. Vous pouvez copier cet ARN pour l'utiliser dans les instructions de la page AWS Policy Generator (Générateur de politique).

   c. Une fois que vous avez fini d'ajouter des instructions, choisissez Generate Policy (Générer une stratégie).
   d. Copiez le texte de stratégie généré, choisissez Fermer et revenez à la page Modifier la stratégie de compartiment dans la console Amazon S3.
7. Dans la zone Politique, modifiez la politique existante ou collez la politique de compartiment depuis le générateur de AWS politiques. Veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions avant d'enregistrer votre stratégie.

   > **Note**
   >
   > Les politiques de compartiment sont limitées à une taille de 20 Ko.

8. Choisissez Save changes (Enregistrer les modifications), ce qui vous ramène à l'onglet Permissions (Autorisations).

À l'aide du AWS SDKs

SDK for Java 2.x

Example

`PutBucketPolicy` AWS SDK for Java 2.x

```
public static void setBucketPolicy(S3Client s3Client, String bucketName, String
 policyText) {

      //sample policy text
      /**
       * policy_statement = {
        *         'Version': '2012-10-17',
        *         'Statement': [
        *             {
        *                 'Sid': 'AdminPolicy',
        *                 'Effect': 'Allow',
        *                 'Principal': {
        *                     "AWS": "111122223333"
        *                 },
        *                 'Action': 's3express:*',
        *                 'Resource':
 'arn:aws:s3express:region:111122223333:bucket/bucket-base-name--zone-id--x-s3'
        *             }
        *         ]
        *     }
        */
        System.out.println("Setting policy:");
        System.out.println("----");
        System.out.println(policyText);
        System.out.println("----");
        System.out.format("On Amazon S3 bucket: \"%s\"\n", bucketName);

        try {
            PutBucketPolicyRequest policyReq = PutBucketPolicyRequest.builder()
                    .bucket(bucketName)
                    .policy(policyText)
                    .build();
```

```
            s3Client.putBucketPolicy(policyReq);
            System.out.println("Done!");
        }

        catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
    }
```

À l'aide du AWS CLI

Cet exemple montre comment créer une politique de compartiment à un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api put-bucket-policy --bucket bucket-base-name--zone-id--x-s3 --policy file://
bucket_policy.json
```

bucket_policy.json :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AdminPolicy",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3express*",
            "Resource": "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-
demo-bucket--usw2-az1--x-s3"
        }
    ]
}
```

Pour de plus amples informations, veuillez consulter put-bucket-policy dans le AWS Command Line Interface.

Affichage d'une politique de compartiment

Pour supprimer une politique pour un compartiment de répertoires, reportez-vous aux exemples suivants.

À l'aide du AWS CLI

Cet exemple montre comment afficher la politique de compartiment attachée à un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *`user input placeholders`* par vos propres informations.

```
aws s3api get-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

Pour de plus amples informations, veuillez consulter get-bucket-policy dans le AWS Command Line Interface.

Suppression d'une politique de compartiment

Pour supprimer une politique pour un compartiment de répertoires, utilisez les exemples suivants.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

`DeleteBucketPolicy` AWS SDK for Java 2.x

```
public static void deleteBucketPolicy(S3Client s3Client, String bucketName) {
      try {
          DeleteBucketPolicyRequest deleteBucketPolicyRequest =
 DeleteBucketPolicyRequest
                  .builder()
                  .bucket(bucketName)
                  .build()
          s3Client.deleteBucketPolicy(deleteBucketPolicyRequest);
          System.out.println("Successfully deleted bucket policy");
      }
```

```
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
```

À l'aide du AWS CLI

Cet exemple montre comment supprimer une politique de compartiment pour un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *`user input placeholders`* par vos propres informations.

```
aws s3api delete-bucket-policy --bucket bucket-base-name--zone-id--x-s3
```

Pour de plus amples informations, veuillez consulter delete-bucket-policy dans le AWS Command Line Interface.

Vidage d'un compartiment de répertoires

Vous pouvez vider un compartiment de répertoires Amazon S3 à l'aide de la console Amazon S3. Pour plus d'informations sur les compartiments de répertoires, consultez Utilisation des compartiments de répertoires.

Avant de vider un compartiment de répertoires, notez les points suivants :

- Lorsque vous videz un compartiment de répertoires, vous supprimez tous les objets, mais vous conservez le compartiment de répertoires.
- Après avoir vidé un compartiment de répertoires, l'action de vidage ne peut pas être annulée.
- Des objets ajoutés au compartiment de répertoires pendant l'action de vidage de compartiment risquent d'être supprimés.

Si vous souhaitez également supprimer le compartiment, notez les points suivants :

- Tous les objets figurant dans le compartiment de répertoires doivent être supprimés avant que le compartiment lui-même puisse être supprimé.
- Les chargements partitionnés en cours dans le compartiment de répertoires doivent être abandonnés avant que le compartiment lui-même puisse être supprimé.

> **Note**
>
> La `s3 rm` commande via la AWS Command Line Interface (CLI), l'`delete`opération via Mountpoint et le bouton d'option Empty bucket via le ne permettent pas de supprimer les téléchargements AWS Management Console partitionnés en cours dans un compartiment de répertoire. Pour supprimer ces chargements partitionnés en cours, utilisez l'opération `ListMultipartUploads` afin d'afficher les chargements partitionnés en cours dans le compartiment et utilisez l'opération `AbortMultipartUpload` pour abandonner tous les chargements partitionnés en cours.

Pour supprimer un compartiment de répertoires, consultez Suppression d'un compartiment de répertoires. Pour abandonner un chargement partitionné en cours, consultez the section called "Interruption d'un chargement partitionné".

Pour vider un compartiment à usage général, consultez Vidange d'un seau à usage général.

Utilisation de la console S3

Pour vider un compartiment de répertoires.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Directory buckets.
3. Choisissez la case d'option située à côté du nom du compartiment à vider, puis choisissez Vider.
4. Dans la page Empty bucket (Vider le compartiment), confirmez que vous souhaitez vider le compartiment en saisissant **`permanently delete`** dans le champ de texte, puis choisissez Empty (Vider).
5. Surveillez la progression du processus de vidage du compartiment sur la page Vider le compartiment : état.

Suppression d'un compartiment de répertoires

Vous ne pouvez supprimer que les compartiments de répertoires Amazon S3 vides. Avant de supprimer votre compartiment de répertoires, vous devez y supprimer tous les objets et abandonner tous les chargements partitionnés en cours.

Si le compartiment de répertoire est attaché à un point d'accès, vous devez d'abord supprimer le point d'accès. Pour de plus amples informations, veuillez consulter Supprimer votre point d'accès pour les compartiments de répertoire.

Pour vider un compartiment de répertoires, consultez Vidage d'un compartiment de répertoires. Pour abandonner un chargement partitionné en cours, consultez the section called "Interruption d'un chargement partitionné".

Pour supprimer un compartiment à usage général, consultez Supprimer un bucket à usage général.

Utilisation de la console S3

Une fois que vous avez vidé votre compartiment de répertoires et que vous avez abandonné tous les chargements partitionnés en cours, vous pouvez supprimer le compartiment.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Directory buckets.
3. Dans la liste Compartiments de répertoires, choisissez la case d'option située à côté du compartiment que vous souhaitez supprimer.
4. Sélectionnez Delete (Supprimer).
5. Sur la page Supprimer le compartiment, saisissez le nom du compartiment dans le champ de texte pour confirmer la suppression de ce compartiment.

   > **Important**
   >
   > La suppression d'un compartiment de répertoires ne peut pas être annulée.

6. Pour supprimer votre compartiment de répertoires, choisissez Supprimer le compartiment.

En utilisant le AWS SDKs

Les exemples suivants suppriment un bucket de répertoire à l'aide des touches AWS SDK for Java 2.x et AWS SDK pour Python (Boto3).

SDK for Java 2.x

Example

```
public static void deleteBucket(S3Client s3Client, String bucketName) {

    try {
        DeleteBucketRequest del = DeleteBucketRequest.builder()
                .bucket(bucketName)
                .build();
        s3Client.deleteBucket(del);
        System.out.println("Bucket " + bucketName + " has been deleted");
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def delete_bucket(s3_client, bucket_name):
    '''
    Delete a directory bucket in a specified Region

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to delete; for example, 'doc-example-bucket--usw2-
az1--x-s3'
    :return: True if bucket is deleted, else False
    '''

    try:
        s3_client.delete_bucket(Bucket = bucket_name)
    except ClientError as e:
        logging.error(e)
        return False
```

```
    return True

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
```

À l'aide du AWS CLI

Cet exemple montre comment créer un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api delete-bucket --bucket bucket-base-name--zone-id--x-s3 --region us-west-2
```

Pour plus d'informations, consultez delete-bucket dans l' AWS Command Line Interface.

Établissement de la liste des compartiments de répertoires

Les exemples suivants montrent comment répertorier les compartiments de répertoires à l'aide des AWS CLI AWS Management Console, AWS SDKs, et.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez afficher la liste de vos compartiments de répertoire.
3. Dans le volet de navigation de gauche, choisissez Directory buckets. La liste des compartiments de répertoire s'affiche. Pour afficher les objets du bucket, les propriétés du bucket, les autorisations du bucket, les métriques, les points d'accès associés au bucket, ou pour gérer le bucket, choisissez le nom du bucket.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

L'exemple suivant affiche la liste des compartiments de répertoires à l'aide du kit AWS SDK for Java 2.x.

```
public static void listBuckets(S3Client s3Client) {
       try {
           ListDirectoryBucketsRequest listDirectoryBucketsRequest =
ListDirectoryBucketsRequest.builder().build();
           ListDirectoryBucketsResponse response =
s3Client.listDirectoryBuckets(listDirectoryBucketsRequest);
           if (response.hasBuckets()) {
               for (Bucket bucket: response.buckets()) {
                   System.out.println(bucket.name());
                   System.out.println(bucket.creationDate());
               }
           }
       }

       catch (S3Exception e) {
           System.err.println(e.awsErrorDetails().errorMessage());
           System.exit(1);
       }
   }
```

SDK for Python

Example

L'exemple suivant affiche la liste des compartiments de répertoires à l'aide du kit AWS SDK pour Python (Boto3).

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_directory_buckets(s3_client):
```

```
    '''
    Prints a list of all directory buckets in a Region

    :param s3_client: boto3 S3 client
    :return: True if there are buckets in the Region, else False
    '''
    try:
        response = s3_client.list_directory_buckets()
        for bucket in response['Buckets']:
            print (bucket['Name'])
    except ClientError as e:
        logging.error(e)
        return False
    return True


    if __name__ == '__main__':
        region = 'us-east-1'
        s3_client = boto3.client('s3', region_name = region)
        list_directory_buckets(s3_client)
```

SDK pour .NET

Example

L'exemple suivant affiche la liste des compartiments de répertoires à l'aide du kit AWS SDK pour .NET.

```
var listDirectoryBuckets = await amazonS3Client.ListDirectoryBucketsAsync(new
 ListDirectoryBucketsRequest
{
  MaxDirectoryBuckets = 10
  }).ConfigureAwait(false);
```

SDK for PHP

Example

L'exemple suivant affiche la liste des compartiments de répertoires à l'aide du kit AWS SDK pour PHP.

```
require 'vendor/autoload.php';

$s3Client = new S3Client([
    'region'      => 'us-east-1',
]);
$result = $s3Client->listDirectoryBuckets();
```

SDK for Ruby

Example

L'exemple suivant affiche la liste des compartiments de répertoires à l'aide du kit AWS SDK pour Ruby.

```
s3 = Aws::S3::Client.new(region:'us-west-1')
s3.list_directory_buckets
```

À l'aide du AWS CLI

L'`list-directory-buckets`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour répertorier vos compartiments de répertoire dans la *`us-east-1`* région. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api list-directory-buckets --region us-east-1
```

Pour plus d'informations, consultez list-directory-buckets dans la Référence des commandes de l'AWS CLI .

Déterminer si vous pouvez accéder à un compartiment de répertoires

Les exemples de AWS SDK suivants montrent comment utiliser l'opération d'`HeadBucket`API pour déterminer si un compartiment d'annuaire Amazon S3 existe et si vous êtes autorisé à y accéder.

En utilisant le AWS SDKs

L' AWS SDK for Java 2.x exemple suivant montre comment déterminer si un bucket existe et si vous êtes autorisé à y accéder.

SDK for Java 2.x

Example

AWS SDK for Java 2.x

```
public static void headBucket(S3Client s3Client, String bucketName) {
   try {
        HeadBucketRequest headBucketRequest = HeadBucketRequest
                .builder()
                .bucket(bucketName)
                .build();
        s3Client.headBucket(headBucketRequest);
        System.out.format("Amazon S3 bucket: \"%s\" found.", bucketName);
   }

   catch (S3Exception e) {
       System.err.println(e.awsErrorDetails().errorMessage());
       System.exit(1);
   }
}
```

À l'aide du AWS CLI

L'exemple `head-bucket` suivant montre comment vous pouvez utiliser l' AWS CLI pour déterminer si un compartiment existe et si vous avez l'autorisation d'y accéder. Pour exécuter cette commande, remplacez les espaces réservés d'entrée utilisateur par vos propres informations.

```
aws s3api head-bucket --bucket bucket-base-name--zone-id--x-s3
```

Pour plus d'informations, consultez head-bucket dans la Référence des commandes de l'AWS CLI .

Utilisation d'objets dans un compartiment de répertoires

Après avoir créé un compartiment d'annuaire Amazon S3, vous pouvez travailler avec des objets à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et du AWS SDKs.

Pour plus d'informations sur l'exécution d'opérations groupées, l'importation, le chargement, la copie, la suppression et le téléchargement d'objets dans des compartiments de répertoires, consultez les rubriques suivantes.

Rubriques

- Importation d'objets dans un compartiment de répertoires
- Utilisation du cycle de vie S3 pour les compartiments de répertoires
- Utilisation des opérations par lots avec les compartiments de répertoires
- Ajout de données à des objets dans des compartiments de répertoires
- Renommer des objets dans des compartiments de répertoires
- Chargement d'objets dans un compartiment de répertoires
- Copie d'objets vers ou depuis un compartiment de répertoires
- Suppression d'objets à partir d'un compartiment de répertoires
- Téléchargement d'un objet à partir d'un compartiment de répertoires
- Génération d'un bucket URLs de répertoire présigné pour partager des objets
- Récupération des métadonnées d'objets à partir de compartiments de répertoires
- Répertorier les objets d'un bucket de répertoire

Importation d'objets dans un compartiment de répertoires

Après avoir créé un compartiment de répertoires dans Amazon S3, vous pouvez remplir le nouveau compartiment avec des données à l'aide de l'action d'importation. L'importation est une méthode simplifiée pour créer des tâches d'opérations par lots S3 afin de copier des objets depuis des compartiments à usage général vers des compartiments de répertoires.

> **Note**
>
> Les limites suivantes s'appliquent aux tâches d'importation :
>
> - Le compartiment source et le compartiment de destination doivent se trouver dans le même Région AWS compte.
> - Le compartiment source ne peut pas être un compartiment de répertoires.
> - Les objets de plus de 5 Go ne sont pas pris en charge et seront omis dans l'opération de copie.

- Les objets des classes de stockage de niveau Glacier Flexible Retrieval, Glacier Deep Archive, Intelligent-Tiering Archive Access et Intelligent-Tiering Deep Archive doivent être restaurés avant de pouvoir être importés.
- Les objets importés avec des algorithmes MD5 de somme de contrôle sont convertis pour utiliser des sommes de CRC32 contrôle.
- Les objets importés utilisent la classe de stockage Express One Zone, dont la structure tarifaire est différente de celle des classes de stockage utilisées par les compartiments à usage général. Tenez compte de cette différence de coût lorsque vous importez un grand nombre d'objets.

Lorsque vous configurez une tâche d'importation, vous spécifiez le compartiment source ou le préfixe source à partir duquel les objets existants seront copiés. Vous fournissez également un rôle AWS Identity and Access Management (IAM) autorisé à accéder aux objets source. Amazon S3 lance ensuite une tâche d'opérations par lots qui copie les objets et applique automatiquement les paramètres de classe de stockage et de somme de contrôle appropriés.

Pour configurer les tâches d'importation, vous utilisez la console Amazon S3.

Utilisation de la console Amazon S3

Pour importer des objets dans un compartiment de répertoires

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments, puis l'onglet Compartiments de répertoires. Choisissez le bouton d'option en regard du compartiment de répertoires dans lequel vous souhaitez importer des objets.
3. Choisissez Importer.
4. Pour Source, entrez le compartiment à usage général (ou le chemin du compartiment, préfixe inclus) qui contient les objets que vous souhaitez importer. Pour choisir un compartiment à usage général existant dans une liste, choisissez Parcourir S3.
5. Pour Autorisation d'accéder aux objets sources et de les copier, effectuez l'une des opérations suivantes pour spécifier un rôle IAM doté des autorisations nécessaires pour importer vos objets sources :

- Pour autoriser Amazon S3 à créer un nouveau rôle IAM en votre nom, choisissez Créer un nouveau rôle IAM.
- Pour choisir un rôle IAM existant dans une liste, choisissez Sélectionner parmi les rôles IAM existants.
- Pour spécifier un rôle IAM existant en entrant son Amazon Resource Name (ARN), choisissez Saisir l'ARN du rôle IAM, puis entrez l'ARN dans le champ correspondant.

6. Passez en revue les informations affichées dans les sections Destination et Paramètres de l'objet copié. Si les informations de la section Destination sont correctes, choisissez Importer pour démarrer la tâche de copie.

   La console Amazon S3 affiche le statut de votre nouvelle tâche sur la page Opérations par lot. Pour plus d'informations sur la tâche, choisissez le bouton d'option à côté du nom de la tâche, puis dans le menu Actions, choisissez Afficher les détails. Pour ouvrir le compartiment de répertoires dans lequel les objets seront importés, choisissez Afficher la destination de l'importation.

Utilisation du cycle de vie S3 pour les compartiments de répertoires

Le cycle de vie S3 vous aide à stocker des objets dans S3 Express One Zone dans des compartiments de répertoires de manière rentable en supprimant les objets ayant expiré en votre nom. Pour gérer le cycle de vie de vos objets, créez une configuration de cycle de vie S3 pour votre compartiment de répertoires. Une configuration de cycle de vie S3 est un ensemble de règles qui définit des actions qu'Amazon S3 applique à un groupe d'objets. Vous pouvez définir une configuration du cycle de vie Amazon S3 sur un compartiment de répertoire à l'aide de l'interface de ligne de AWS commande (AWS CLI) AWS SDKs, de l'API REST Amazon S3 et AWS CloudFormation.

Dans votre configuration du cycle de vie, utilisez des règles pour définir les actions que vous souhaitez qu'Amazon S3 effectue au niveau de vos objets. Pour les objets stockés dans des compartiments de répertoires, vous pouvez créer des règles de cycle de vie pour faire expirer les objets à mesure que le temps passe. Vous pouvez également créer des règles de cycle de vie pour supprimer les chargements partitionnés incomplets dans les compartiments de répertoire à une fréquence quotidienne.

Quand vous ajoutez une configuration de cycle de vie dans un compartiment, les règles de configuration s'appliquent à la fois aux objets existants et à ceux que vous ajouterez ultérieurement.

À titre d'exemple, si vous ajoutez aujourd'hui une règle de configuration du cycle de vie avec une action qui entraîne l'expiration des objets dotés d'un préfixe spécifique 30 jours après leur création, S3 mettra dans la file d'attente pour suppression tous les objets de plus de 30 jours qui incluent le préfixe spécifié.

En quoi le cycle de vie S3 des compartiments de répertoires est différent

Pour les objets qui se trouvent dans des compartiments de répertoires, vous pouvez créer des règles de cycle de vie pour faire expirer ces objets et supprimer les chargements partitionnés incomplets. Toutefois, le cycle de vie S3 des compartiments de répertoires ne prend pas en charge les actions de transition entre les classes de stockage.

CreateSession

Le cycle de vie utilise des opérations d'API `DeleteObject` et `DeleteObjects` publiques pour faire expirer les objets dans les compartiments de répertoires. Pour utiliser ces opérations d'API, le cycle de vie S3 utilise l'API `CreateSession` afin d'établir des informations d'identification de sécurité temporaires pour accéder aux objets qui se trouvent dans les compartiments de répertoires. Pour plus d'informations, consultez `CreateSession` dans la Référence d'API Amazon S3.

Si vous avez une politique active qui refuse les autorisations de suppression au principal du cycle de vie, cela vous empêche d'autoriser le cycle de vie S3 à supprimer des objets en votre nom.

Utilisation d'une politique de compartiment pour accorder des autorisations au principal du service de cycle de vie S3

La politique de compartiment suivante autorise les CreateSession appels avec la `ReadWrite` session par défaut et autorise le principal du service de cycle de vie.

Example – Politique de compartiment permettant d'autoriser les appels **`CreateSession`** avec la session **`ReadWrite`** par défaut

```
{
  "Version":"2008-10-17",
  "Statement":[
     {
        "Effect":"Allow",
        "Principal": {
           "Service":"lifecycle.s3.amazonaws.com"
         },
```

```
          "Action":"s3express:CreateSession",
          "Condition": {
             "StringEquals": {
                "s3express:SessionMode": "ReadWrite"
              }
           },
           "Resource":"arn:aws:s3express:us-east-2:412345678921:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
       }
   ]
}
```

Surveillance des règles de cycle de vie

Pour les objets stockés dans des compartiments de répertoire, S3 Lifecycle génère AWS CloudTrail des journaux d'événements de gestion et de données. Pour plus d'informations, consultez les exemples de fichiers CloudTrail journaux pour S3 Express One Zone.

Pour plus d'informations sur la création de la configuration d'un cycle de vie et sur la résolution des problèmes liés au cycle de vie S3, consultez les rubriques suivantes :

Rubriques

- Création et gestion d'une configuration de cycle de vie pour votre compartiment de répertoires
- Résolution des problèmes liés au cycle de vie S3 pour les compartiments de répertoires

Création et gestion d'une configuration de cycle de vie pour votre compartiment de répertoires

Vous pouvez créer une configuration du cycle de vie pour les compartiments de répertoire en utilisant the AWS Command Line Interface (AWS CLI) AWS SDKs et REST APIs.

Utilisation de la AWS CLI

Vous pouvez utiliser les AWS CLI commandes suivantes pour gérer les configurations du cycle de vie S3 :

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

Pour obtenir des instructions sur la configuration du AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

Notez que la configuration de cycle de vie Amazon S3 est un fichier XML. Mais lorsque vous utilisez le AWS CLI, vous ne pouvez pas spécifier le format XML. Vous devez spécifier le format JSON à la place. Vous trouverez ci-dessous des exemples de configurations de cycle de vie XML et les configurations JSON équivalentes que vous pouvez spécifier dans une AWS CLI commande.

L'exemple de AWS CLI suivant place une politique de configuration du cycle de vie dans un compartiment de répertoire. Cette politique spécifie que tous les objets dont le préfixe est labelisé (myprefix) et qui correspondent à la taille définie expirent après 7 jours. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

Enregistrez la stratégie de configuration du cycle de vie dans un fichier JSON. Dans cet exemple, le fichier est nommé lifecycle1.json.

Example

JSON

```
{
    "Rules": [
        {
        "Expiration": {
            "Days": 7
        },
        "ID": "Lifecycle expiration rule",
        "Filter": {
            "And": {
                "Prefix": "myprefix/",
                "ObjectSizeGreaterThan": 500,
                "ObjectSizeLessThan": 64000
            }
        },
        "Status": "Enabled"
    }
    ]
}
```

Envoyez le fichier JSON en tant que partie de la commande CLI `put-bucket-lifecycle-configuration`. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations.

```
aws s3api put-bucket-lifecycle-configuration --region us-west-2 --profile default
 --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 --lifecycle-configuration file://lc-
policy.json --checksum-algorithm crc32c
```

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>Lifecycle expiration rule</ID>
        <Filter>
            <And>
                <Prefix>myprefix/</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        <Expiration>
             <Days>7</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

En utilisant le AWS SDKs

SDK for Java

Example

```
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationRequest;
import
 software.amazon.awssdk.services.s3.model.PutBucketLifecycleConfigurationResponse;
import software.amazon.awssdk.services.s3.model.ChecksumAlgorithm;
import software.amazon.awssdk.services.s3.model.BucketLifecycleConfiguration;
import software.amazon.awssdk.services.s3.model.LifecycleRule;
import software.amazon.awssdk.services.s3.model.LifecycleRuleFilter;
import software.amazon.awssdk.services.s3.model.LifecycleExpiration;
import software.amazon.awssdk.services.s3.model.LifecycleRuleAndOperator;
```

```
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationResponse;
import
 software.amazon.awssdk.services.s3.model.GetBucketLifecycleConfigurationRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleRequest;
import software.amazon.awssdk.services.s3.model.DeleteBucketLifecycleResponse;
import software.amazon.awssdk.services.s3.model.AbortIncompleteMultipartUpload;

// PUT a Lifecycle policy
LifecycleRuleFilter objectExpirationFilter =
 LifecycleRuleFilter.builder().and(LifecycleRuleAndOperator.builder().prefix("dir1/").object
LifecycleRuleFilter mpuExpirationFilter =
 LifecycleRuleFilter.builder().prefix("dir2/").build();

LifecycleRule objectExpirationRule =
 LifecycleRule.builder().id("lc").filter(objectExpirationFilter).status("Enabled").expiratio
                    .days(10)
                    .build())
                .build();
LifecycleRule mpuExpirationRule = LifecycleRule.builder().id("lc-
mpu").filter(mpuExpirationFilter).status("Enabled").abortIncompleteMultipartUpload(AbortInco
                        .daysAfterInitiation(10)
                        .build())
                .build();

PutBucketLifecycleConfigurationRequest putLifecycleRequest =
 PutBucketLifecycleConfigurationRequest.builder()
                .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3")
                .checksumAlgorithm(ChecksumAlgorithm.CRC32)
                .lifecycleConfiguration(
                        BucketLifecycleConfiguration.builder()
                                .rules(objectExpirationRule, mpuExpirationRule)
                                .build()
                ).build();

PutBucketLifecycleConfigurationResponse resp =
 client.putBucketLifecycleConfiguration(putLifecycleRequest);

// GET the Lifecycle policy
GetBucketLifecycleConfigurationResponse getResp =
 client.getBucketLifecycleConfiguration(GetBucketLifecycleConfigurationRequest.builder().buc
s3-demo-bucket--usw2-az1--x-s3").build());

// DELETE the Lifecycle policy
```

```
DeleteBucketLifecycleResponse delResp =
 client.deleteBucketLifecycle(DeleteBucketLifecycleRequest.builder().bucket("amzn-
s3-demo-bucket--usw2-az1--x-s3").build());
```

SDK for Go

Example

```
package main

import (
    "context"
    "log"

    "github.com/aws/aws-sdk-go-v2/aws"
    "github.com/aws/aws-sdk-go-v2/config"
    "github.com/aws/aws-sdk-go-v2/service/s3"
    "github.com/aws/aws-sdk-go-v2/service/s3/types"
)
// PUT a Lifecycle policy
func putBucketLifecycleConfiguration(client *s3.Client, bucketName string ) error {
    lifecycleConfig := &s3.PutBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
        LifecycleConfiguration: &types.BucketLifecycleConfiguration{
            Rules: []types.LifecycleRule{
                {
                    ID:     aws.String("lc"),
                    Filter: &types.LifecycleRuleFilter{
                        And: &types.LifecycleRuleAndOperator{
                            Prefix: aws.String("foo/"),
                            ObjectSizeGreaterThan: aws.Int64(1000000),
                            ObjectSizeLessThan:    aws.Int64(100000000),
                            },
                        },

                    Status: types.ExpirationStatusEnabled,
                    Expiration: &types.LifecycleExpiration{
                        Days: aws.Int32(int32(1)),
                    },
                },
                {
                    ID:     aws.String("abortmpu"),
                    Filter: &types.LifecycleRuleFilter{
                        Prefix: aws.String("bar/"),
```

```
                    },
                    Status: types.ExpirationStatusEnabled,
                    AbortIncompleteMultipartUpload:
 &types.AbortIncompleteMultipartUpload{
                        DaysAfterInitiation: aws.Int32(int32(5)),
                    },
                },
            },
        },
    }
    _, err := client.PutBucketLifecycleConfiguration(context.Background(),
 lifecycleConfig)
    return err
}
// Get the Lifecycle policy
func getBucketLifecycleConfiguration(client *s3.Client, bucketName string) error {
    getLifecycleConfig := &s3.GetBucketLifecycleConfigurationInput{
        Bucket: aws.String(bucketName),
    }

    resp, err := client.GetBucketLifecycleConfiguration(context.Background(),
 getLifecycleConfig)
    if err != nil {
        return err
    }
    return nil
}
// Delete the Lifecycle policy
func deleteBucketLifecycleConfiguration(client *s3.Client, bucketName string) error
 {
    deleteLifecycleConfig := &s3.DeleteBucketLifecycleInput{
        Bucket: aws.String(bucketName),
    }
    _, err := client.DeleteBucketLifecycle(context.Background(),
 deleteLifecycleConfig)
    return err
}
func main() {
    cfg, err := config.LoadDefaultConfig(context.Background(),
 config.WithRegion("us-west-2")) // Specify your region here
    if err != nil {
        log.Fatalf("unable to load SDK config, %v", err)
    }
    s3Client := s3.NewFromConfig(cfg)
```

```
    bucketName := "amzn-s3-demo-bucket--usw2-az1--x-s3"
    putBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
    deleteBucketLifecycleConfiguration(s3Client, bucketName)
    getBucketLifecycleConfiguration(s3Client, bucketName)
}
```

SDK for .NET

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "amzn-s3-demo-bucket--usw2-az1--x-s3";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List <LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "delete rule",
```

```
                                Filter = new LifecycleFilter()
                                {
                                    LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                    {
                                        Prefix = "projectdocs/"
                                    }
                                },
                                Status = LifecycleRuleStatus.Enabled,
                                Expiration = new LifecycleRuleExpiration()
                                {
                                      Days = 10
                                }
                            }
                        }
                };

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "mpu abort rule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 10
                    },
                    AbortIncompleteMultipartUpload = new
LifecycleRuleAbortIncompleteMultipartUpload()
                    {
                        DaysAfterInitiation = 10
                    }
```

```
                });

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now two rules.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=2; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }
```

```
        static async Task <LifecycleConfiguration>
 RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
            GetLifecycleConfigurationRequest request = new
 GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
 DeleteLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
        }
    }
}
```

SDK for Python

Example

```
import boto3

client = boto3.client("s3", region_name="us-west-2")
bucket_name = 'amzn-s3-demo-bucket--usw2-az1--x-s3'

client.put_bucket_lifecycle_configuration(
    Bucket=bucket_name,
    ChecksumAlgorithm='CRC32',
    LifecycleConfiguration={
        'Rules': [
            {
                'ID': 'lc',
                'Filter': {
                    'And': {
```

```
                        'Prefix': 'foo/',
                        'ObjectSizeGreaterThan': 1000000,
                        'ObjectSizeLessThan': 100000000,
                    }
                },
                'Status': 'Enabled',
                'Expiration': {
                    'Days': 1
                }
            },
            {
                'ID': 'abortmpu',
                'Filter': {
                    'Prefix': 'bar/'
                },
                'Status': 'Enabled',
                'AbortIncompleteMultipartUpload': {
                    'DaysAfterInitiation': 5
                }
            }
        ]
    }
)

result = client.get_bucket_lifecycle_configuration(
    Bucket=bucket_name
)

client.delete_bucket_lifecycle(
    Bucket=bucket_name
)
```

Résolution des problèmes liés au cycle de vie S3 pour les compartiments de répertoires

Rubriques

- J'ai spécifié la configuration de mon cycle de vie, mais les objets de mon compartiment de répertoires n'expirent pas
- Comment puis-je surveiller les actions prises conformément à mes règles de cycle de vie ?

J'ai spécifié la configuration de mon cycle de vie, mais les objets de mon compartiment de répertoires n'expirent pas

S3 Lifecycle pour les compartiments d'annuaire utilise le public APIs pour supprimer des objets dans S3 Express One Zone. Pour utiliser le public au niveau de l'objet APIs, vous devez autoriser S3 Lifecycle à supprimer vos objets `CreateSession` et autoriser S3 Lifecycle à le supprimer. Si vous avez une politique active qui refuse les autorisations de suppression, cela vous empêche d'autoriser le cycle de vie S3 à supprimer des objets en votre nom.

Il est important de configurer correctement vos politiques de compartiment afin de garantir que les objets que vous souhaitez supprimer sont éligibles à l'expiration. Vous pouvez consulter les AWS CloudTrail journaux de `AccessDenied` Trails for `CreateSession` API invocations CloudTrail afin de vérifier si l'accès a été refusé. La vérification de vos CloudTrail journaux peut vous aider à résoudre les problèmes d'accès et à identifier la cause première des erreurs de refus d'accès. Vous pouvez ensuite corriger les contrôles d'accès incorrects en mettant à jour les politiques pertinentes.

Si vous confirmez que les politiques de vos compartiments sont correctement définies et que vous rencontrez toujours des problèmes, nous vous recommandons de vérifier les règles du cycle de vie pour vous assurer qu'elles sont appliquées au sous-ensemble d'objets approprié.

Comment puis-je surveiller les actions prises conformément à mes règles de cycle de vie ?

Vous pouvez utiliser AWS CloudTrail les journaux d'événements de données pour surveiller les actions entreprises par S3 Lifecycle dans les compartiments de répertoire. Pour plus d'informations, consultez les exemples de fichiers CloudTrail journaux.

Utilisation des opérations par lots avec les compartiments de répertoires

Vous pouvez utiliser les opérations par lots Amazon S3 pour effectuer des opérations sur des objets stockés dans des compartiments S3. Pour en savoir plus sur les opérations par lots S3, consultez Exécution des opérations par lots à grande échelle sur des objets Amazon S3.

Les rubriques suivantes traitent de l'exécution d'opérations par lot sur des objets stockés dans des compartiments de répertoires pour la classe de stockage S3 Express One Zone.

Rubriques

- Utilisation des opérations par lots avec les compartiments de répertoires
- Principales différences

Utilisation des opérations par lots avec les compartiments de répertoires

Vous pouvez effectuer les opérations Copier et Invoquer la fonction AWS Lambda sur des objets stockés dans des compartiments de répertoires. Avec la fonction Copier, vous pouvez copier des objets entre des compartiments du même type (par exemple, d'un compartiment de répertoires à un autre). Vous pouvez également copier entre des compartiments à usage général et des compartiments de répertoires. Avec AWS Lambda la fonction Invoke, vous pouvez utiliser une fonction Lambda pour effectuer des actions sur les objets de votre bucket de répertoire avec le code que vous définissez.

Copie d'objets

Vous pouvez copier entre des compartiments de même type ou entre des compartiments de répertoires et des compartiments à usage général. Lorsque vous effectuez une copie vers un compartiment de répertoires, vous devez utiliser le format d'Amazon Resource Name (ARN) approprié pour ce type de compartiment. Le format d'ARN d'un compartiment de répertoires est `arn:aws:s3express:`*`region`*`:`*`account-id`*`:bucket/`*`bucket-base-name`*`--x-s3`.

> **Note**
>
> La copie d'objets entre différents Régions AWS n'est pas prise en charge lorsque le compartiment source ou de destination se trouve dans une zone AWS locale. Les compartiments source et de destination doivent avoir la même Région AWS parent. Les compartiments source et de destination peuvent correspondre à différents types d'emplacement de compartiment (zone de disponibilité ou zone locale).

Vous pouvez également remplir votre compartiment de répertoires avec des données à l'aide de l'action Importer de la console S3. L'action Importer est une méthode simplifiée pour créer des tâches d'opérations par lots afin de copier des objets depuis des compartiments à usage général vers des compartiments de répertoires. Pour les tâches de copie Importer depuis des compartiments à usage général vers des compartiments de répertoires, S3 génère automatiquement un manifeste. Pour plus d'informations, consultez Importation d'objets dans un compartiment de répertoires et Spécification d'un manifeste.

Invocation de fonctions Lambda (**`LambdaInvoke`**)

L'utilisation d'opérations par lots pour invoquer des fonctions Lambda agissant sur des compartiments de répertoires est soumise à des exigences particulières. Par exemple, vous

devez structurer votre demande Lambda à l'aide d'un schéma d'invocation JSON v2 et spécifier InvocationSchemaVersion 2.0 lorsque vous créez la tâche. Pour plus d'informations, consultez Invoquer une fonction AWS Lambda.

Principales différences

Voici la liste des principales différences lors de l'utilisation des opérations par lot pour effectuer des opérations groupées sur des objets stockés dans des compartiments de répertoires avec la classe de stockage S3 Express One Zone :

- Pour les compartiments d'annuaire, le SSE-S3 et le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) sont pris en charge. Si vous effectuez une demande `CopyObject` qui spécifie d'utiliser le chiffrement côté serveur avec des clés fournies par le client (SSE-C) sur un compartiment de répertoires (source ou cible), la réponse renverra une erreur HTTP `400 (Bad Request)`.

  Nous recommandons que le chiffrement par défaut du compartiment utilise la configuration de chiffrement souhaitée et que vous ne remplaciez pas le chiffrement par défaut du compartiment dans vos demandes `CreateSession` ni dans vos demandes d'objets PUT. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. Pour plus d'informations sur les comportements de contournement du chiffrement dans les compartiments de répertoire et sur la façon de chiffrer les nouvelles copies d'objets dans un compartiment d'annuaire avec SSE-KMS, voir Spécification du chiffrement côté serveur avec pour les téléchargements de nouveaux objets. AWS KMS

  Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de l'opération Copy dans les opérations par lot. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS. Pour plus d'informations sur l'utilisation de SSE-KMS au niveau des compartiments de répertoires, consultez Configuration et surveillance du chiffrement par défaut pour les compartiments de répertoires et Utilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de répertoire.
- Les objets figurant dans des compartiments de répertoires ne peuvent pas être balisés. Vous ne pouvez spécifier qu'un jeu de balises vide. Par défaut, les opérations par lots copient les balises. Si vous copiez un objet comportant des balises entre des compartiments à usage général et des compartiments de répertoires, vous recevrez une réponse `501 (Not Implemented)`.

- S3 Express One Zone vous offre la possibilité de choisir l'algorithme de somme de contrôle utilisé pour valider vos données pendant le chargement ou le téléchargement. Vous pouvez sélectionner l'un des algorithmes de hachage sécurisé (SHA) ou de contrôle de redondance cyclique (CRC) suivants : CRC32, CRC32 SHA-1 et SHA-256. MD5les checksums basés sur la base de données ne sont pas pris en charge avec la classe de stockage S3 Express One Zone.
- Par défaut, tous les compartiments Amazon S3 définissent le paramètre S3 Object Ownership comme étant appliqué par le propriétaire du compartiment et les listes de contrôle d'accès (ACLs) sont désactivées. Pour les compartiments de répertoires, ce paramètre ne peut pas être modifié. Vous pouvez copier un objet à partir de compartiments à usage général vers des compartiments de répertoires. Cependant, vous ne pouvez pas remplacer la liste ACL par défaut lorsque vous effectuez une copie vers ou depuis un compartiment de répertoires.
- Quelle que soit la manière dont vous spécifiez votre manifeste, la liste elle-même doit être stockée dans un compartiment à usage général. Les opérations par lots ne peuvent pas importer de manifestes existants à partir de compartiments de répertoires, ni enregistrer les manifestes générés dans ces compartiments. Toutefois, les objets décrits dans le manifeste peuvent être stockés dans des compartiments de répertoires.
- Les opérations par lots ne peuvent pas spécifier un compartiment de répertoires comme emplacement dans un rapport d'inventaire S3. Les rapports d'inventaire ne prennent pas en charge les compartiments de répertoires. Vous pouvez créer un fichier manifeste pour les objets d'un compartiment de répertoires en utilisant l'API `ListObjectsV2` pour répertorier les objets. Vous pouvez ensuite insérer cette liste dans un fichier CSV.

Octroi d'accès

Pour effectuer des tâches de copie, vous devez disposer des autorisations suivantes :

- Pour copier des objets d'un compartiment de répertoires vers un autre, vous devez disposer de l'autorisation `s3express:CreateSession`.
- Pour copier des objets à partir de compartiments de répertoires vers des compartiments à usage général, vous devez disposer de l'autorisation `s3express:CreateSession` et de l'autorisation `s3:PutObject` permettant d'écrire la copie des objets dans le compartiment de destination.
- Pour copier des objets dans des compartiments de répertoires à partir de compartiments à usage général, vous devez disposer de l'autorisation `s3express:CreateSession` et de l'autorisation `s3:GetObject` permettant de lire l'objet source à copier.

Pour plus d'informations, consultez CopyObject dans la Référence d'API Amazon Simple Storage Service.

- Pour invoquer une fonction Lambda, vous devez accorder des autorisations à votre ressource sur la base de votre fonction Lambda. Vérifiez les autorisations d'API correspondantes pour déterminer quelles autorisations sont requises.

Ajout de données à des objets dans des compartiments de répertoires

Vous pouvez ajouter des données à la fin des objets existants stockés dans la classe de stockage S3 Express One Zone dans les compartiments de répertoires. Nous vous recommandons d'utiliser la fonctionnalité permettant d'ajouter des données à un objet si les données sont écrites en continu pendant une période de temps spécifique ou si vous devez lire l'objet pendant que vous y ajoutez des données. L'ajout de données à des objets est courant dans des cas d'utilisation tels que l'ajout de nouvelles entrées de journal aux fichiers journaux ou l'ajout de nouveaux segments vidéo aux fichiers vidéo lors de leur transcodage puis de leur diffusion en continu. En ajoutant des données aux objets, vous pouvez simplifier les applications qui combinaient auparavant les données dans le stockage local avant de copier l'objet final sur Amazon S3.

Aucune taille minimale n'est requise pour les données que vous pouvez ajouter à un objet. Toutefois, la taille maximale des données que vous pouvez ajouter à un objet dans une seule demande est de 5 Go. Il s'agit de la même limite que la taille de demande la plus grande lors du chargement de données à l'aide d'une API Amazon S3.

À chaque opération d'ajout réussie, vous créez une partie de l'objet, et chaque objet peut comporter jusqu'à 10 000 parties. Vous pouvez donc ajouter une entité de données à un objet jusqu'à 10 000 fois. Si un objet est créé à l'aide du chargement partitionné S3, chaque partie chargée est prise en compte dans le calcul du quota maximum de 10 000 parties. Par exemple, vous pouvez ajouter jusqu'à 9 000 parties à un objet créé par chargement partitionné comprenant 1 000 parties.

> **Note**
>
> Si vous atteignez la limite de pièces, vous recevrez un TooManyPartsmessage d'erreur. Vous pouvez utiliser l'API `CopyObject` pour réinitialiser le décompte.

Si vous souhaitez charger des parties dans un objet en parallèle et que vous n'avez pas besoin de les lire pendant le chargement, nous vous recommandons d'utiliser le chargement partitionné Amazon S3. Pour plus d'informations, consultez Utilisation du chargement partitionné.

L'ajout de données aux objets n'est pris en charge que pour les objets qui se trouvent dans des compartiments de répertoires stockés dans la classe de stockage S3 Express One Zone. Pour plus d'informations sur S3 Express One Zone, consultez Bien démarrer avec S3 Express One Zone.

Pour commencer à ajouter des données aux objets de vos compartiments de répertoire, vous pouvez utiliser la AWS SDKs AWS CLI et l'`PutObject`API. Lorsque vous effectuez une demande `PutObject`, vous définissez l'en-tête `x-amz-write-offset-bytes` en fonction de la taille de l'objet auquel vous ajoutez des données. Pour utiliser l'opération d'API `PutObject`, vous devez utiliser l'API `CreateSession` afin d'établir des informations d'identification de sécurité temporaires pour accéder aux objets de vos compartiments de répertoires. Pour plus d'informations, consultez `PutObject` et `CreateSession` dans la Référence d'API Amazon S3.

Chaque opération d'ajout réussie est facturée comme une demande `PutObject`. Pour en savoir plus sur la tarification, consultez `Amazon S3 pricing`.

> **Note**
>
> À partir de la version 1.12, Mountpoint pour Amazon S3 prend en charge l'ajout de données aux objets stockés dans S3 Express One Zone. Pour commencer, vous devez d'abord activer cette fonctionnalité en définissant l'indicateur `--incremental-upload` . Pour plus d'informations sur Mountpoint, consultez Utilisation de Mountpoint.

Si vous utilisez un algorithme CRC (Cyclic Redundancy Check) lors du chargement des données ajoutées, vous pouvez récupérer les sommes de contrôle CRC de l'objet entier à l'aide de la demande `HeadObject` ou `GetObject`. Si vous utilisez l'algorithme SHA-1 ou SHA-256 lors du téléchargement des données ajoutées, vous pouvez récupérer une somme de contrôle des parties ajoutées et vérifier leur intégrité à l'aide des sommes de contrôle SHA renvoyées lors des réponses précédentes. PutObject Pour plus d'informations, consultez Protection et chiffrement des données.

Ajout de données à vos objets à l'aide de la AWS CLI AWS SDKs et de l'API REST

Vous pouvez ajouter des données à vos objets à l'aide de l'API AWS Command Line Interface (AWS CLI) AWS SDKs et de l'API REST.

Utilisation de la AWS CLI

L'`put-object`exemple de commande suivant montre comment utiliser la AWS CLI pour ajouter des données à un objet. Pour exécuter cette commande, remplacez le *`user input placeholders`* par vos propres informations

```
aws s3api put-object --bucket amzn-s3-demo-bucket--azid--x-s3 --key sampleinput/
file001.bin --body bucket-seed/file001.bin --write-offset-bytes size-of-sampleinput/
file001.bin
```

En utilisant le AWS SDKs

SDK for Java

Vous pouvez utiliser le AWS SDK pour Java pour ajouter des données à vos objets.

```
var putObjectRequestBuilder = PutObjectRequest.builder()
                                              .key(key)
                                              .bucket(bucketName)
                                              .writeOffsetBytes(9);
var response = s3Client.putObject(putObjectRequestBuilder.build());
```

SDK for Python

```
s3.put_object(Bucket='amzn-s3-demo-bucket--use2-az2--x-s3', Key='2024-11-05-sdk-
test', Body=b'123456789', WriteOffsetBytes=9)
```

Utilisation de l'API REST

Vous pouvez envoyer des demandes REST pour ajouter des données à un objet. Pour de plus amples informations, veuillez consulter `PutObject`.

Renommer des objets dans des compartiments de répertoires

À l'aide de cette `RenameObject` opération, vous pouvez renommer automatiquement un objet existant dans un compartiment de répertoire qui utilise la classe de stockage S3 Express One Zone, sans aucun mouvement de données. Vous pouvez renommer un objet en spécifiant le nom de l'objet existant comme source et le nouveau nom de l'objet comme destination dans le même compartiment de répertoire. L'opération `RenameObject` d'API ne réussira pas sur les objets qui se terminent par le caractère séparateur slash (`/`). Pour plus d'informations, consultez Nommer les objets Amazon S3.

L'`RenameObject`opération est généralement terminée en quelques millisecondes, quelle que soit la taille de l'objet. Cette fonctionnalité accélère les applications telles que la gestion des fichiers journaux, le traitement multimédia et l'analyse des données. En outre, `RenameObject` préserve toutes les propriétés des métadonnées des objets, notamment la classe de stockage, le type de chiffrement, la date de création, la date de dernière modification et les propriétés de somme de contrôle.

> **Note**
>
> `RenameObject`n'est pris en charge que pour les objets stockés dans la classe de stockage S3 Express One Zone.

Pour accorder l'accès à l'`RenameObject`opération, nous vous recommandons d'utiliser l'`CreateSession`opération pour une autorisation basée sur la session. Plus précisément, vous accordez l'`s3express:CreateSession`autorisation au compartiment d'annuaire dans le cadre d'une politique de compartiment ou d'une politique basée sur l'identité. Ensuite, vous devez effectuer l'appel `CreateSession` d'API sur le bucket de répertoire pour obtenir un jeton de session. Avec le jeton de session dans l'en-tête de votre demande, vous pouvez envoyer des requêtes d'API à cette opération. Une fois le jeton de session expiré, vous effectuez un autre appel d'`CreateSession`API pour générer un nouveau jeton de session à utiliser. La AWS CLI créera et AWS SDKs gérera votre session, notamment en actualisant automatiquement le jeton de session pour éviter les interruptions de service lorsqu'une session expire. Pour plus d'informations sur l'autorisation, consultez `CreateSession`le manuel Amazon S3 API Reference. Pour en savoir plus sur les opérations de l'API des points de terminaison zonaux, consultez la section Autorisation des opérations de l'API des points de terminaison zonaux avec. `CreateSession`

Si vous ne souhaitez pas remplacer un objet existant, vous pouvez ajouter l'en-tête `If-None-Match` conditionnel avec la valeur de `'*'` la `RenameObject` demande. Amazon S3 renvoie une `412 Precondition Failed` erreur si le nom de l'objet existe déjà. Pour plus d'informations, consultez `RenameObject` dans la Référence d'API Amazon S3.

`RenameObject`est une opération d'API de point de terminaison zonal (opération au niveau de l'objet ou du plan de données) à laquelle est enregistrée. AWS CloudTrail Vous pouvez l'utiliser CloudTrail pour recueillir des informations sur les `RenameObject` opérations effectuées sur vos objets dans des compartiments de répertoire. Pour plus d'informations, consultez la section Journalisation avec AWS CloudTrail pour les compartiments de répertoire et les exemples de fichiers CloudTrail journaux pour les compartiments de répertoire.

S3 Express One Zone est la seule classe de stockage qui prend en charge`RenameObject`, au même prix que`PUT`, `COPY`POST, et les `LIST` demandes (pour 1 000 demandes) dans S3 Express One Zone. Pour plus d'informations, consultez Tarification Amazon S3.

Modification du nom d'un objet

Pour renommer un objet dans votre compartiment de répertoire, vous pouvez utiliser la console Amazon S3, la AWS CLI AWS SDKs, l'API REST ou Mountpoint pour Amazon S3 (version 1.19.0 ou ultérieure).

Utilisation de la console S3

Pour renommer un objet dans un bucket de répertoire

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Buckets, puis cliquez sur l'onglet Buckets du répertoire. Accédez au compartiment de répertoire Amazon S3 qui contient l'objet que vous souhaitez renommer.
3. Cochez la case située à côté de l'objet que vous voulez renommer.
4. Dans le menu Actions, sélectionnez Renommer l'objet.
5. Dans la zone Nouveau nom d'objet, saisissez le nouveau nom de l'objet.

> **Note**
>
> Si vous spécifiez le même nom d'objet qu'un objet existant, l'opération échouera et Amazon S3 renvoie un `412 Precondition Failed` message d'erreur. La longueur du nom de la clé de l'objet ne peut pas dépasser 1 024 octets. Les préfixes inclus dans le nom de l'objet sont pris en compte dans la longueur totale.

6. Choisissez Renommer l'objet. Amazon S3 renommera votre objet.

Utilisation de la AWS CLI

Les `rename-object` exemples montrent comment vous pouvez utiliser la AWS CLI pour renommer un objet. Pour exécuter ces commandes, remplacez le *`user input placeholders`* par vos propres informations

L'exemple suivant montre comment renommer un objet avec une vérification conditionnelle sur celui de ETag l'objet source.

```
aws s3api rename-object \
    --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 \
    --key new-file.txt \
    --rename-source amzn-s3-demo-bucket--usw2-az1--x-s3/original-file.txt \
    --source-if-match "\"a1b7c3d2e5f6\""
```

Cette commande exécute les opérations suivantes :

- Renomme un objet de *original-file.txt* à *new-file.txt* dans le compartiment de *amzn-s3-demo-bucket--usw2-az1--x-s3* répertoire.
- N'effectue le changement de nom que si l'objet source ETag correspond à « *a1b7c3d4e5f6* ».

Si ce ETag n'est pas le cas, l'opération échouera avec une `412 Precondition Failed` erreur.

L'exemple suivant montre comment renommer un objet à l'aide d'une vérification conditionnelle du nouveau nom d'objet spécifié.

```
aws s3api rename-object \
    --bucket amzn-s3-demo-bucket--usw2-az1--x-s3 \
    --key new-file.txt \
    --rename-source amzn-s3-demo-bucket--usw2-az1--x-s3/original-file.txt \
    --destination-if-none-match "\"e5f3g7h8i9j0\""
```

Cette commande exécute les opérations suivantes :

- Renomme un objet de *original-file.txt* à *new-file.txt* dans le compartiment de *amzn-s3-demo-bucket--usw2-az1--x-s3* répertoire.
- N'exécute l'opération de renommage que si l'objet existe et que celui de l'objet ETag ne correspond pas à « *e5f3g7h8i9j0* ».

Si un objet existe déjà avec le nouveau nom spécifié et la correspondance ETag, l'opération échouera avec une `412 Precondition Failed` erreur.

En utilisant le AWS SDKs

SDK for Java

Vous pouvez utiliser le AWS SDK pour Java pour renommer vos objets. Pour utiliser ces exemples, remplacez le *`user input placeholders`* par vos propres informations

L'exemple suivant montre comment créer un à `RenameObjectRequest` l'aide du AWS SDK for Java

```
String key = "key";
String newKey = "new-key";
String expectedETag = "e5f3g7h8i9j0";
RenameObjectRequest renameRequest = RenameObjectRequest.builder()
    .bucket(amzn-s3-demo-bucket--usw2-az1--x-s3)
    .key(newKey)
    .renameSource(key)
    .destinationIfMatch(e5f3g7h8i9j0)
    .build();
```

Ce code effectue les opérations suivantes :

- Créez une demande pour renommer un objet de « » en *`key`* « *`new-key`* » dans le compartiment de *`amzn-s3-demo-bucket--usw2-az1--x-s3`* répertoire.
- Inclut une condition selon laquelle le changement de nom ne sera effectué que si l'objet ETag correspond à « *`e5f3g7h8i9j0`* ».
- Si le ETag ne correspond pas ou si l'objet n'existe pas, l'opération échouera.

L'exemple suivant montre comment créer une `RenameObjectRequest` condition sans correspondance à l'aide du AWS SDK for Java.

```
String key = "key";
String newKey = "new-key";
String noneMatchETag = "e5f3g7h8i9j0";
RenameObjectRequest renameRequest = RenameObjectRequest.builder()
    .bucket(amzn-s3-demo-bucket--usw2-az1--x-s3)
    .key(newKey)
    .renameSource(key)
    .destinationIfNoneMatch(noneMatchETag)
    .build();
```

Ce code effectue les opérations suivantes :

- Crée une demande pour renommer un objet de « *key* » à « *new-key* » dans le compartiment de *amzn-s3-demo-bucket--usw2-az1--x-s3* répertoire.
- Inclut une condition qui garantit `.destinationIfNoneMatch(noneMatchETag)` que le changement de nom n'aura lieu que si celui de l'objet de destination ETag ne correspond pas à « *e5f3g7h8i9j0* ».

L'opération échouera avec une `412 Precondition Failed` erreur si un objet existe avec le nouveau nom spécifié et porte le nom spécifié ETag.

SDK for Python

Vous pouvez utiliser le SDK pour Python pour renommer vos objets. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

L'exemple suivant montre comment renommer un objet à l'aide du AWS SDK pour Python (Boto3).

```
def basic_rename(bucket, source_key, destination_key):
    try:
        s3.rename_object(
            Bucket=amzn-s3-demo-bucket--usw2-az1--x-s3,
            Key=destination_key,
            RenameSource=f"{amzn-s3-demo-bucket--usw2-az1--x-s3}/{source_key}"
        )
        print(f"Successfully renamed {source_key} to {destination_key}")
    except ClientError as e:
        print(f"Error renaming object: {e}")
```

Ce code effectue les opérations suivantes :

- Renomme un objet de *source_key* à *destination_key* dans le compartiment de *amzn-s3-demo-bucket--usw2-az1--x-s3* répertoire.
- Imprime un message de réussite si le changement de nom de votre objet est réussi ou un message d'erreur s'il échoue.

L'exemple suivant montre comment renommer un objet avec les `DestinationIfNoneMatch` conditions `SourceIfMatch` et à l'aide du AWS SDK pour Python (Boto3).

```
def rename_with_conditions(bucket, source_key, destination_key, source_etag,
 dest_etag):
    try:
        s3.rename_object(
            Bucket=amzn-s3-demo-bucket--usw2-az1--x-s3,
            Key=destination_key,
            RenameSource=f"{amzn-s3-demo-bucket--usw2-az1--x-s3}/{source_key}",
            SourceIfMatch=source_ETag,
            DestinationIfNoneMatch=dest_ETag
        )
        print(f"Successfully renamed {source_key} to {destination_key} with
 conditions")
    except ClientError as e:
        print(f"Error renaming object: {e}")
```

Ce code effectue les opérations suivantes :

- Effectue une opération de renommage conditionnel et applique deux conditions, `SourceIfMatch` et`DestinationIfNoneMatch`. La combinaison de ces conditions garantit que l'objet n'a pas été modifié et qu'aucun objet n'existe déjà avec le nouveau nom spécifié.
- Renomme un objet de *source_key* à *destination_key* dans le compartiment de *amzn-s3-demo-bucket--usw2-az1--x-s3* répertoire.
- Imprime un message de réussite si le changement de nom de votre objet est réussi, ou imprime un message d'erreur en cas d'échec ou si les conditions ne sont pas remplies.

SDK for Rust

Vous pouvez utiliser le SDK pour Rust pour renommer vos objets. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

L'exemple suivant montre comment renommer un objet dans le bucket de *amzn-s3-demo-bucket--usw2-az1--x-s3* répertoire à l'aide du SDK pour Rust.

```
async fn basic_rename_example(client: &Client) -> Result<(), Box<dyn Error>> {
    let response = client
        .rename_object()
        .bucket(" amzn-s3-demo-bucket--usw2-az1--x-s3")
        .key("new-name.txt")  // New name/path for the object
        .rename_source("old-name.txt")  // Original object name/path
        .send()
```

```
        .await?;
    Ok(())
}
```

Ce code effectue les opérations suivantes :

- Crée une demande pour renommer un objet de « *old-name.tx* » à « *new-name.txt* » dans le compartiment de *amzn-s3-demo-bucket--usw2-az1--x-s3* répertoire.
- Renvoie un `Result` type pour gérer les erreurs potentielles.

Utilisation de l'API REST

Vous pouvez envoyer des requêtes REST pour renommer un objet. Pour plus d'informations, consultez `RenameObject` dans la Référence d'API Amazon S3.

Utilisation de Mountpoint pour Amazon S3

À partir de la version 1.19.0 ou supérieure, Mountpoint pour Amazon S3 permet de renommer les objets dans S3 Express One Zone. Pour plus d'informations sur Mountpoint, consultez Utilisation de Mountpoint.

Chargement d'objets dans un compartiment de répertoires

Après avoir créé un compartiment de répertoires Amazon S3, vous pouvez y charger des objets. Les exemples suivants montrent comment télécharger un objet dans un compartiment de répertoire à l'aide de la console S3 et du AWS SDKs. Pour plus d'informations sur les opérations d'objet par lot utilisant S3 Express One Zone, consultez Gestion des objets.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Directory buckets.
3. Choisissez le nom du compartiment dans lequel vous souhaitez charger vos dossiers ou fichiers.
4. Dans l'onglet Objets, choisissez Charger.
5. Sur la page Charger, procédez de l'une des manières suivantes :

    - Faites glisser et déposez les fichiers et les dossiers dans la fenêtre de chargement.

- Choisissez Ajouter des fichiers ou Ajouter un dossier, puis choisissez les fichiers ou les dossiers à charger et sélectionnez Ouvrir ou Charger.

6. Sous Sommes de contrôle, choisissez la fonction de somme de contrôle que vous souhaitez utiliser.

   (Facultatif) Si vous chargez un seul objet d'une taille inférieure à 16 Mo, vous pouvez également spécifier une valeur de somme de contrôle précalculée. Lorsque vous fournissez une valeur précalculée, Amazon S3 la compare à la valeur qu'il calcule à l'aide de la fonction de somme de contrôle sélectionnée. Si les valeurs ne correspondent pas, le chargement ne démarrera pas.

7. Les options des sections Autorisations et Propriétés sont automatiquement définies selon les paramètres par défaut et ne peuvent pas être modifiées. Le blocage de l'accès public est automatiquement activé, et la gestion des versions S3 ainsi que le verrouillage d'objet S3 ne peuvent pas être activés pour les compartiments de répertoires.

   (Facultatif) Si vous souhaitez ajouter des métadonnées sous forme de paires clé-valeur aux objets, développez la section Propriétés, puis dans la section Métadonnées, choisissez Ajouter des métadonnées.

8. Pour charger les fichiers et dossiers répertoriés, choisissez Charger.

   Amazon S3 charge les objets et les dossiers. Lorsque le chargement est terminé, un message de réussite s'affiche sur la page Charger : statut.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

```
public static void putObject(S3Client s3Client, String bucketName, String objectKey,
 Path filePath) {
       //Using File Path to avoid loading the whole file into memory
       try {
           PutObjectRequest putObj = PutObjectRequest.builder()
                   .bucket(bucketName)
                   .key(objectKey)
                   //.metadata(metadata)
                   .build();
           s3Client.putObject(putObj, filePath);
```

```
            System.out.println("Successfully placed " + objectKey +" into bucket
 "+bucketName);

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
}
```

SDK for Python

Example

```
import boto3
import botocore
from botocore.exceptions import ClientError


def put_object(s3_client, bucket_name, key_name, object_bytes):
    """
    Upload data to a directory bucket.
    :param s3_client: The boto3 S3 client
    :param bucket_name: The bucket that will contain the object
    :param key_name: The key of the object to be uploaded
    :param object_bytes: The data to upload
    """
    try:
        response = s3_client.put_object(Bucket=bucket_name, Key=key_name,
                            Body=object_bytes)
        print(f"Upload object '{key_name}' to bucket '{bucket_name}'.")
        return response
    except ClientError:
        print(f"Couldn't upload object '{key_name}' to bucket '{bucket_name}'.")
        raise

def main():
    # Share the client session with functions and objects to benefit from S3 Express
 One Zone auth key
    s3_client = boto3.client('s3')
    # Directory bucket name must end with --zone-id--x-s3
    resp = put_object(s3_client, 'doc-bucket-example--use1-az5--x-s3', 'sample.txt',
 b'Hello, World!')
```

```
    print(resp)

if __name__ == "__main__":
    main()
```

À l'aide du AWS CLI

L'exemple de commande `put-object` suivant montre comment utiliser l'interface de ligne de commande AWS CLI pour charger un objet depuis Amazon S3. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key sampleinut/
file001.bin --body bucket-seed/file001.bin
```

Pour plus d'informations, consultez put-object dans la Référence des commandes de l'AWS CLI .

Rubriques

- Utilisation du chargement partitionné avec les compartiments de répertoires

Utilisation du chargement partitionné avec les compartiments de répertoires

Vous pouvez utiliser le chargement partitionné pour charger un seul objet en tant qu'ensemble de parties. Chaque partie est une portion contiguë des données de l'objet. Vous pouvez charger ces parties d'objet indépendamment et dans n'importe quel ordre. Si le transfert d'une partie échoue, vous pouvez la retransférer sans affecter les autres. Une fois toutes les parties de l'objet chargées, Amazon S3 les assemble et crée l'objet. En général, lorsque l'objet atteint la taille de 100 Mo, vous devez préférer les chargements partitionnés au chargement d'objet en une seule opération.

L'utilisation du chargement partitionné offre les avantages suivants :

- Meilleur débit : vous pouvez charger des parties en parallèle pour améliorer le débit.
- Quick recovery from any network issues (Récupération rapide après des problèmes réseau) — la taille réduite des parties minimise l'impact du redémarrage d'un chargement qui a échoué en raison d'une erreur réseau.
- Pause and resume object uploads (Interruption et reprise des chargements d'objet) — vous pouvez charger des parties d'objet au fil du temps. Après le lancement d'un chargement partitionné, il n'y a aucune date d'expiration. Vous devez explicitement finaliser ou abandonner le chargement partitionné.

- Begin an upload before you know the final object size (Lancement d'un chargement avant de connaître la taille finale de l'objet) — vous pouvez charger un objet à mesure que vous le créez.

Nous vous recommandons d'utiliser le chargement partitionné comme suit :

- Si vous chargez des objets volumineux sur un réseau à large bande passante stable, utilisez le chargement partitionné pour optimiser l'utilisation de la bande passante disponible en chargeant des parties d'objet en parallèle pour bénéficier de performances multithreads.
- Si vous effectuez un chargement sur un réseau irrégulier, utilisez le chargement partitionné pour augmenter la résilience aux erreurs réseau en évitant les redémarrages du chargement. Lorsque vous utilisez le chargement partitionné, vous n'avez besoin de relancer le chargement que pour les parties d'objet dont le chargement a été interrompu. Vous n'avez pas besoin de redémarrer le chargement de vos objets depuis le début.

Lorsque vous utilisez des chargements partitionnés pour charger des objets vers la classe de stockage Amazon S3 Express One Zone dans des compartiments de répertoire, le processus est similaire au processus d'utilisation du chargement partitionné pour charger des objets dans des compartiments à usage général. Cependant, il existe quelques différences importantes.

Pour plus d'informations sur l'utilisation du chargement partitionné pour charger des objets dans S3 Express One Zone, consultez les rubriques suivantes.

Rubriques

- Processus de chargement partitionné
- Totaux de contrôle avec les opérations de chargement partitionné
- Opérations simultanées de chargement partitionné
- Chargement partitionné et tarification
- Opérations de l'API de chargement partitionné et autorisations
- Exemples

Processus de chargement partitionné

Un chargement partitionné est un processus en trois étapes :

- Vous lancez le chargement.
- Vous chargez les parties de l'objet.

- Une fois que vous avez chargé toutes les parties, vous pouvez finaliser le chargement partitionné.

Dès réception de la demande de finalisation du chargement partitionné, Amazon S3 crée l'objet à partir des parties chargées pour que vous puissiez ensuite y accéder comme vous le feriez avec n'importe quel autre objet du compartiment.

Lancement du chargement partitionné

Lorsque vous envoyez une demande pour lancer un chargement partitionné, Amazon S3 renvoie une réponse avec un ID de chargement, qui est un identifiant unique pour le chargement partitionné. Vous devez inclure cet ID de chargement dès que vous chargez les parties, listez les parties, terminez un chargement ou interrompez un chargement.

Chargement de parties

Lorsque vous chargez une partie, outre l'ID de chargement, vous devez spécifier un numéro de partie. Lorsque vous utilisez le chargement partitionné avec S3 Express One Zone, les numéros de chaque partie du chargement doivent être consécutifs. Si vous essayez d'effectuer une demande de chargement partitionné avec des numéros de partie non consécutifs, une erreur `HTTP 400 Bad Request` (ordre non valide) est générée.

Un numéro de partie identifie de manière unique une partie et sa place dans l'objet que vous chargez. Si vous chargez une nouvelle partie avec le même numéro qu'une partie précédemment chargée, cette dernière sera écrasée.

Chaque fois que vous chargez une partie, Amazon S3 renvoie un en-tête entity tag (ETag) dans sa réponse. Pour chaque téléchargement partiel, vous devez enregistrer le numéro de pièce et la ETag valeur. Les ETag valeurs de tous les chargements de parties d'objets resteront les mêmes, mais un numéro de pièce différent sera attribué à chaque partie. Vous devez inclure ces valeurs dans la demande ultérieure pour terminer le chargement partitionné.

Amazon S3 chiffre automatiquement tous les nouveaux objets chargés dans un compartiment S3. Dans le cadre d'un chargement partitionné, si vous ne spécifiez pas d'informations de chiffrement dans votre demande, le paramètre de chiffrement des parties chargées est défini sur la configuration de chiffrement par défaut du compartiment de destination. La configuration de chiffrement par défaut d'un compartiment Amazon S3 est toujours activée et est au minimum définie sur le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3). Pour les compartiments d'annuaire, le SSE-S3 et le chiffrement côté serveur avec AWS KMS clés (SSE-KMS) sont pris en charge. Pour de plus amples informations, veuillez consulter Protection et chiffrement des données.

Fin du chargement partitionné

Lorsque vous terminez un chargement partitionné, Amazon S3 crée l'objet en concaténant les parties par ordre croissant en fonction des numéros de partie. À l'issue d'une demande de chargement complet, les parties n'existent plus.

Votre demande complète de téléchargement en plusieurs parties doit inclure l'ID de téléchargement et une liste des deux numéros de pièce et de leurs ETag valeurs correspondantes. La réponse Amazon S3 inclut un ETag identifiant unique les données d'objet combinées. Il ne ETag s'agit pas d'un MD5 hachage des données de l'objet.

Listes de chargement partitionné

Vous pouvez lister les parties d'un chargement partitionné spécifique ou de tous les chargements partitionnés en cours. L'opération de liste des parties renvoie des informations sur les parties que vous avez chargées pour un chargement partitionné spécifique. Pour chaque demande de liste des parties, Amazon S3 renvoie des informations sur les parties pour le chargement partitionné spécifié, pour 1 000 parties maximum. Si le chargement partitionné compte plus de 1 000 parties, vous devez utiliser la pagination pour récupérer toutes les parties.

La liste des parties retournée n'inclut pas les parties qui n'ont pas fini d'être chargées. En utilisant l'opération d'affichage des chargements partitionnés, vous pouvez obtenir la liste des chargements partitionnés qui sont en cours.

Un chargement partitionné en cours est un chargement que vous avez lancé, mais que vous n'avez pas encore terminé ou interrompu. Chaque demande renvoie 1 000 chargements partitionnés maximum. S'il y a plus de 1 000 chargements partitionnés en cours, vous devez envoyer des demandes supplémentaires pour récupérer les chargements partitionnés restants. Utilisez la liste renvoyée uniquement pour la vérification. N'utilisez pas le résultat de la liste lorsque vous envoyez une requête de chargement partitionné complet. Conservez plutôt votre propre liste des numéros de pièce que vous avez spécifiés lors du chargement des pièces et des ETag valeurs correspondantes renvoyées par Amazon S3.

Pour plus d'informations sur les listes de chargement partitionné, consultez ListParts dans la Référence d'API Amazon Simple Storage Service.

Totaux de contrôle avec les opérations de chargement partitionné

Lorsque vous chargez un objet vers, vous pouvez spécifier un algorithme de somme de contrôle pour vérifier l'intégrité de l'objet. MD5 n'est pas pris en charge pour les compartiments de répertoire. Vous

pouvez spécifier l'un des algorithmes suivants de contrôle de l'intégrité des données, Secure Hash Algorithms (SHA) ou Cyclic Redundancy Check (CRC) :

- CRC32
- CRC32 C
- SHA-1
- SHA-256

Vous pouvez utiliser l'API REST Amazon S3 ou AWS SDKs pour récupérer la valeur de la somme de contrôle pour des parties individuelles en utilisant `GetObject` ou`HeadObject`. Pour récupérer les valeurs de contrôle des parties individuelles de téléchargements partitionnés toujours en cours, vous pouvez utiliser `ListParts`.

> **Important**
>
> Lorsque vous utilisez les algorithmes de somme de contrôle précédents, les numéros de chaque partie du chargement partitionné doivent être consécutifs. Si vous essayez d'effectuer une demande de chargement partitionné avec des numéros de partie non consécutifs, Amazon S3 génère une erreur `HTTP 400 Bad Request` (ordre non valide).

Pour plus d'informations sur le fonctionnement des sommes de contrôle avec les objets d'un chargement partitionné, consultez Vérification de l'intégrité des objets dans Amazon S3.

Opérations simultanées de chargement partitionné

Dans un environnement de développement distribué, l'application peut lancer plusieurs mises à jour sur le même objet en même temps. Par exemple, l'application peut lancer plusieurs chargements partitionnés à l'aide de la même clé d'objet. Pour chacun de ces chargements, l'application peut ensuite charger des parties et envoyer une demande de chargement complet à Amazon S3 pour créer l'objet. Pour S3 Express One Zone, l'instant de création de l'objet correspond à la date d'achèvement du chargement partitionné.

> **Important**
>
> La gestion des versions n'est pas prise en charge pour les objets stockés dans les compartiments de répertoires.

Chargement partitionné et tarification

Lorsque vous lancez un chargement partitionné, Amazon S3 conserve toutes les parties jusqu'à ce que vous terminiez ou annuliez le chargement. Tout au long de sa durée de vie, le stockage, la bande passante et les demandes pour ce chargement partitionné ainsi que ses parties associées vous sont facturés. Si vous abandonnez le chargement partitionné, S3 supprime les artefacts de chargement et les parties que vous avez chargées, et ils ne vous sont plus facturés. Aucuns frais de suppression anticipée ne sont facturés pour la suppression de chargements partitionnés incomplets, quelle que soit la classe de stockage spécifiée. Pour plus d'informations sur la tarification, consultez Tarification Amazon S3.

> **Important**
>
> Si la demande de finalisation du chargement partitionné n'est pas envoyée correctement, les parties de l'objet ne sont pas assemblées et aucun objet n'est créé. Vous êtes facturé pour tout le stockage associé aux parties chargées. Il est donc important de finaliser le chargement partitionné pour que l'objet soit créé, ou d'annuler le chargement partitionné pour supprimer les parties déjà chargées.
>
> Avant de supprimer un compartiment de répertoires, vous devez finaliser ou annuler tous les chargements partitionnés en cours. Les compartiments de répertoires ne prennent pas en charge les configurations de cycle de vie S3. Si nécessaire, vous pouvez répertorier vos chargements partitionnés actifs, puis annuler les chargements et supprimer votre compartiment.

Opérations de l'API de chargement partitionné et autorisations

Pour autoriser l'accès aux opérations d'API de gestion des objets sur un compartiment de répertoires, vous accordez l'autorisation `s3express:CreateSession` dans un compartiment de répertoires ou une politique basée sur l'identité AWS Identity and Access Management (IAM).

Vous devez posséder les autorisations nécessaires pour utiliser les opérations de chargement partitionné. Vous pouvez utiliser des politiques de compartiment ou des politiques basées sur l'identité IAM pour accorder aux principaux IAM les autorisations nécessaires pour effectuer ces opérations. Le tableau suivant répertorie les autorisations nécessaires pour diverses opérations de chargement partitionné.

Vous pouvez identifier l'initiateur d'un chargement partitionné avec l'élément `Initiator`. Si l'initiateur est un Compte AWS, cet élément fournit les mêmes informations que l'0wnerélément. Si l'initiateur est un utilisateur IAM, cet élément fournit l'ARN utilisateur et le nom complet.

Action	Autorisations requises
Créer un chargement partitionné	Pour créer un chargement partitionné, vous devez être autorisé à effectuer l'action `s3express:CreateSession` sur le compartiment de répertoires.
Lancement d'un chargement partitionné	Pour lancer un chargement partitionné, vous devez être autorisé à effectuer l'action `s3express:CreateSession` sur le compartiment de répertoires.
Chargement d'une partie	Pour charger une partie, vous devez être autorisé à effectuer l'action `s3express:CreateSession` sur le compartiment de répertoires. Le propriétaire du compartiment doit autoriser l'initiateur à effectuer l'action `s3express:CreateSession` sur le compartiment de répertoires pour que l'initiateur charge une partie.
Chargement d'une partie (copie)	Pour charger une partie, vous devez être autorisé à effectuer l'action `s3express:CreateSession` sur le compartiment de répertoires. Pour que l'initiateur puisse charger une partie pour un objet, le propriétaire du compartiment doit l'autoriser à effectuer l'action `s3express:CreateSession` sur l'objet.
Terminer un chargement partitionné	Pour finaliser un chargement partitionné, vous devez être autorisé à effectuer l'action `s3express:CreateSession` au niveau du compartiment de répertoires. Le propriétaire du compartiment doit autoriser l'initiateur à effectuer l'action `s3express:CreateSession` sur l'objet pour que l'initiateur puisse finaliser un chargement partitionné.
Abandonner un	Pour abandonner un chargement partitionné, vous devez être autorisé à exécuter l'action `s3express:CreateSession` .

Action	Autorisations requises
chargement partitionné	Pour annuler un chargement partitionné, son initiateur doit avoir obtenu une autorisation d'accès explicite pour effectuer l'action `s3express:CreateSession` .
Liste des parties	Pour répertorier les parties d'un chargement partitionné, vous devez être autorisé à effectuer l'action `s3express:CreateSession` sur le compartiment de répertoires.
Lister des chargements partitionnés en cours	Pour répertorier les chargements partitionnés en cours dans un compartiment, vous devez être autorisé à exécuter l'action `s3:ListBucketMultipartUploads` au niveau de ce compartiment.

Prise en charge des opérations d'API pour le chargement partitionné

Les sections suivantes de la Référence d'API Amazon Simple Storage Service décrivent les opérations d'API REST Amazon S3 pour les chargement partitionnés.

- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- AbortMultipartUpload
- ListParts
- ListMultipartUploads

Exemples

Pour charger un objet dans S3 Express One Zone dans un compartiment de répertoires à l'aide du chargement partitionné, consultez les exemples suivants.

Rubriques

- Création d'un chargement partitionné
- Chargement des parties d'un chargement partitionné

- Achèvement d'un chargement partitionné
- Interruption d'un chargement partitionné
- Création d'une opération de copie d'un chargement partitionné
- Affichage de la liste des chargements partitionnés en cours
- Affichage de la liste des parties d'un chargement partitionné

Création d'un chargement partitionné

> **Note**
>
> Pour les compartiments de répertoires, lorsque vous effectuez une opération `CreateMultipartUpload` et une opération `UploadPartCopy`, le chiffrement par défaut du compartiment doit utiliser la configuration de chiffrement souhaitée, et les en-têtes de demande que vous fournissez dans la demande `CreateMultipartUpload` doivent correspondre à la configuration de chiffrement par défaut du compartiment de destination.

Les exemples suivants montrent comment créer un chargement partitionné.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts
 *
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--use1-az4--x-s3'
 * @param key
 * @return
 */
 private static String createMultipartUpload(S3Client s3, String bucketName, String
 key) {

     CreateMultipartUploadRequest createMultipartUploadRequest =
 CreateMultipartUploadRequest.builder()
```

```
            .bucket(bucketName)
            .key(key)
            .build();

    String uploadId = null;

    try {
        CreateMultipartUploadResponse response =
s3.createMultipartUpload(createMultipartUploadRequest);
        uploadId = response.uploadId();
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
    return uploadId;
```

SDK for Python

Example

```
def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
   Create a multipart upload to a directory bucket

   :param s3_client: boto3 S3 client
   :param bucket_name: The destination bucket for the multipart upload
   :param key_name: The key name for the object to be uploaded
   :return: The UploadId for the multipart upload if created successfully, else None
   '''

   try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None
```

À l'aide du AWS CLI

Cet exemple montre comment créer un chargement partitionné pour un compartiment de répertoires à l'aide de l' AWS CLI. Cette commande lance un téléchargement partitionné vers le compartiment de répertoire *bucket-base-name zone-id* --x-s3 pour l'objet. *KEY_NAME* Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api create-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME
```

Pour de plus amples informations, veuillez consulter create-multipart-upload dans le AWS Command Line Interface.

Chargement des parties d'un chargement partitionné

Les exemples suivants montrent comment charger les parties d'un chargement partitionné.

En utilisant le AWS SDKs

SDK for Java 2.x

L'exemple suivant montre comment diviser un objet unique en plusieurs parties, puis comment les charger dans un compartiment de répertoires à l'aide du kit SDK pour Java 2.x.

Example

```
/**
 * This method creates part requests and uploads individual parts to S3 and then
 returns all the completed parts
 *
 * @param s3
 * @param bucketName
 * @param key
 * @param uploadId
 * @throws IOException
 */
 private static ListCompletedPartmultipartUpload(S3Client s3, String bucketName,
 String key, String uploadId, String filePath) throws IOException {

        int partNumber = 1;
        ListCompletedPart completedParts = new ArrayList<>();
        ByteBuffer bb = ByteBuffer.allocate(1024 * 1024 * 5); // 5 MB byte buffer
```

```
        // read the local file, breakdown into chunks and process
        try (RandomAccessFile file = new RandomAccessFile(filePath, "r")) {
            long fileSize = file.length();
            int position = 0;
            while (position < fileSize) {
                file.seek(position);
                int read = file.getChannel().read(bb);

                bb.flip(); // Swap position and limit before reading from the
buffer.
                UploadPartRequest uploadPartRequest = UploadPartRequest.builder()
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .partNumber(partNumber)
                        .build();

                UploadPartResponse partResponse = s3.uploadPart(
                        uploadPartRequest,
                        RequestBody.fromByteBuffer(bb));

                CompletedPart part = CompletedPart.builder()
                        .partNumber(partNumber)
                        .eTag(partResponse.eTag())
                        .build();
                completedParts.add(part);

                bb.clear();
                position += read;
                partNumber++;
            }
        }

        catch (IOException e) {
            throw e;
        }
        return completedParts;
    }
```

SDK for Python

L'exemple suivant montre comment diviser un objet unique en plusieurs parties, puis comment les charger dans un compartiment de répertoires à l'aide du kit SDK pour Python.

Example

```
def multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_size):
    '''
    Break up a file into multiple parts and upload those parts to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name for object to be uploaded and for the local file
 that's being uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_size: The size parts that the object will be broken into, in bytes.
                      Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
 last part of your multipart upload.
    :return: part_list for the multipart upload if all parts are uploaded
 successfully, else None
    '''

    part_list = []
    try:
        with open(key_name, 'rb') as file:
            part_counter = 1
            while True:
                file_part = file.read(part_size)
                if not len(file_part):
                    break
                upload_part = s3_client.upload_part(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = mpu_id,
                    Body = file_part,
                    PartNumber = part_counter
                )
                part_list.append({'PartNumber': part_counter, 'ETag':
 upload_part['ETag']})
                part_counter += 1
    except ClientError as e:
        logging.error(e)
        return None
    return part_list
```

À l'aide du AWS CLI

Cet exemple montre comment diviser un seul objet en plusieurs parties, puis comment charger ces parties dans un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api upload-part --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --part-number 1 --body LOCAL_FILE_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

Pour plus d'informations, consultez upload-part dans l' AWS Command Line Interface.

Achèvement d'un chargement partitionné

Les exemples suivants montrent comment finaliser un chargement partitionné.

En utilisant le AWS SDKs

SDK for Java 2.x

Les exemples suivants montrent comment finaliser un chargement partitionné à l'aide du kit SDK pour Java 2.x.

Example

```
/**
 * This method completes the multipart upload request by collating all the upload
 parts
 * @param s3
 * @param bucketName - for example, 'doc-example-bucket--usw2-az1--x-s3'
 * @param key
 * @param uploadId
 * @param uploadParts
 */
 private static void completeMultipartUpload(S3Client s3, String bucketName, String
 key, String uploadId, ListCompletedPart uploadParts) {
        CompletedMultipartUpload completedMultipartUpload =
 CompletedMultipartUpload.builder()
                .parts(uploadParts)
                .build();

        CompleteMultipartUploadRequest completeMultipartUploadRequest =
                CompleteMultipartUploadRequest.builder()
```

```
                        .bucket(bucketName)
                        .key(key)
                        .uploadId(uploadId)
                        .multipartUpload(completedMultipartUpload)
                        .build();

        s3.completeMultipartUpload(completeMultipartUploadRequest);
    }

    public static void multipartUploadTest(S3Client s3, String bucketName, String
 key, String localFilePath)  {
        System.out.println("Starting multipart upload for: " + key);
        try {
            String uploadId = createMultipartUpload(s3, bucketName, key);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUpload(s3, bucketName, key, uploadId,
 localFilePath);
            completeMultipartUpload(s3, bucketName, key, uploadId, parts);
            System.out.println("Multipart upload completed for: " + key);
        }

        catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

Les exemples suivants montrent comment finaliser un chargement partitionné à l'aide du kit SDK pour Python.

Example

```
def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: The destination bucket for the multipart upload
    :param key_name: The key name for the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: The list of uploaded part numbers with their associated ETags
```

```
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'OBJECT_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_upload(s3_client, bucket_name, key_name, mpu_id,
 part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id,
 part_list):
                print (f'{key_name} successfully uploaded through a ultipart upload
 to {bucket_name}')
            else:
                print (f'Could not upload {key_name} hrough a multipart upload to
 {bucket_name}')
```

À l'aide du AWS CLI

Cet exemple montre comment finaliser un chargement partitionné pour un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *`user input placeholders`* par vos propres informations.

```
aws s3api complete-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
 --multipart-upload file://parts.json
```

Cet exemple utilise une structure JSON qui décrit les parties du chargement partitionné qui doivent être réassemblées dans le fichier complet. Dans cet exemple, le préfixe `file://` est utilisé pour charger la structure JSON à partir d'un fichier du dossier local nommé `parts`.

parts.json :

```
parts.json
{
  "Parts": [
    {
      "ETag": "6b78c4a64dd641a58dac8d9258b88147",
      "PartNumber": 1
    }
  ]
}
```

Pour de plus amples informations, veuillez consulter complete-multipart-upload dans le AWS Command Line Interface.

Interruption d'un chargement partitionné

Les exemples suivants montrent comment abandonner un chargement partitionné.

En utilisant le AWS SDKs

SDK for Java 2.x

L'exemple suivant montre comment abandonner un chargement partitionné à l'aide du kit SDK pour Java 2.x.

Example

```
public static void abortMultiPartUploads( S3Client s3, String bucketName ) {

         try {
             ListMultipartUploadsRequest listMultipartUploadsRequest =
 ListMultipartUploadsRequest.builder()
```

```
                    .bucket(bucketName)
                    .build();

            ListMultipartUploadsResponse response =
 s3.listMultipartUploads(listMultipartUploadsRequest);
            ListMultipartUpload uploads = response.uploads();

            AbortMultipartUploadRequest abortMultipartUploadRequest;
            for (MultipartUpload upload: uploads) {
                abortMultipartUploadRequest = AbortMultipartUploadRequest.builder()
                        .bucket(bucketName)
                        .key(upload.key())
                        .uploadId(upload.uploadId())
                        .build();

                s3.abortMultipartUpload(abortMultipartUploadRequest);
            }

        }

        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

L'exemple suivant montre comment abandonner un chargement partitionné à l'aide du kit SDK pour Python.

Example

```
import logging
import boto3
from botocore.exceptions import ClientError


def abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
    '''
    Aborts a partial multipart upload in a directory bucket.

    :param s3_client: boto3 S3 client
```

```
    :param bucket_name: Bucket where the multipart upload was initiated - for
 example, 'doc-example-bucket--usw2-az1--x-s3'
    :param key_name: Name of the object for which the multipart upload needs to be
 aborted
    :param upload_id: Multipart upload ID for the multipart upload to be aborted
    :return: True if the multipart upload was successfully aborted, False if not
    '''
    try:
        s3_client.abort_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = upload_id
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
        upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    if abort_multipart_upload(s3_client, bucket_name, key_name, upload_id):
        print (f'Multipart upload for object {key_name} in {bucket_name} bucket has
 been aborted')
    else:
        print (f'Unable to abort multipart upload for object {key_name} in
 {bucket_name} bucket')
```

À l'aide du AWS CLI

Les exemples suivants montrent comment abandonner un chargement partitionné à l'aide de l'AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api abort-multipart-upload --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME --upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
MAQAAAAB0OxUFeA7LTbWWFS8WYwhrxDxTIDN-pdEEq_agIHqsbg"
```

Pour de plus amples informations, veuillez consulter abort-multipart-upload dans le AWS Command Line Interface.

Création d'une opération de copie d'un chargement partitionné

> **Note**
>
> - Pour chiffrer de nouvelles copies partielles d'objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. Votre configuration SSE-KMS ne peut prendre en charge qu'une seule clé gérée par le client par compartiment de répertoires pendant toute la durée de vie du compartiment. Après avoir spécifié une clé gérée par le client pour SSE-KMS, vous ne pouvez pas remplacer cette clé pour la configuration SSE-KMS du compartiment. Vous ne pouvez pas spécifier de paramètres de chiffrement côté serveur pour les nouvelles copies partielles d'objets avec SSE-KMS dans les en-têtes de demande. UploadPartCopy En outre, les en-têtes de demande que vous fournissez dans la demande `CreateMultipartUpload` doivent correspondre à la configuration de chiffrement par défaut du compartiment de destination.
> - Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de l'opération UploadPartCopy. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS.

Les exemples suivants montrent comment copier des objets d'un compartiment vers un autre à l'aide du chargement partitionné.

En utilisant le AWS SDKs

SDK for Java 2.x

L'exemple suivant montre comment utiliser un chargement partitionné pour copier un objet par programmation d'un compartiment à un autre à l'aide du kit SDK pour Java 2.x.

Example

```
/**
 * This method creates a multipart upload request that generates a unique upload ID
 that is used to track
 * all the upload parts.
 *
 * @param s3
 * @param bucketName
 * @param key
 * @return
 */
 private static String createMultipartUpload(S3Client s3, String bucketName, String
 key) {
        CreateMultipartUploadRequest createMultipartUploadRequest =
 CreateMultipartUploadRequest.builder()
                .bucket(bucketName)
                .key(key)
                .build();
        String uploadId = null;
        try {
            CreateMultipartUploadResponse response =
 s3.createMultipartUpload(createMultipartUploadRequest);
            uploadId = response.uploadId();
        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }
        return uploadId;
  }

  /**
   * Creates copy parts based on source object size and copies over individual parts
   *
   * @param s3
   * @param sourceBucket
   * @param sourceKey
   * @param destnBucket
   * @param destnKey
   * @param uploadId
   * @return
   * @throws IOException
   */
```

```
   public static ListCompletedPart multipartUploadCopy(S3Client s3, String
sourceBucket, String sourceKey, String destnBucket, String destnKey, String
uploadId) throws IOException {

       // Get the object size to track the end of the copy operation.
       HeadObjectRequest headObjectRequest = HeadObjectRequest
               .builder()
               .bucket(sourceBucket)
               .key(sourceKey)
               .build();
       HeadObjectResponse response = s3.headObject(headObjectRequest);
       Long objectSize = response.contentLength();

       System.out.println("Source Object size: " + objectSize);

       // Copy the object using 20 MB parts.
       long partSize = 20 * 1024 * 1024;
       long bytePosition = 0;
       int partNum = 1;
       ListCompletedPart completedParts = new ArrayList<>();
       while (bytePosition < objectSize) {
           // The last part might be smaller than partSize, so check to make sure
           // that lastByte isn't beyond the end of the object.
           long lastByte = Math.min(bytePosition + partSize - 1, objectSize - 1);

           System.out.println("part no: " + partNum + ", bytePosition: " +
bytePosition + ", lastByte: " + lastByte);

           // Copy this part.
           UploadPartCopyRequest req = UploadPartCopyRequest.builder()
                   .uploadId(uploadId)
                   .sourceBucket(sourceBucket)
                   .sourceKey(sourceKey)
                   .destinationBucket(destnBucket)
                   .destinationKey(destnKey)
                   .copySourceRange("bytes="+bytePosition+"-"+lastByte)
                   .partNumber(partNum)
                   .build();
           UploadPartCopyResponse res = s3.uploadPartCopy(req);
           CompletedPart part = CompletedPart.builder()
                   .partNumber(partNum)
                   .eTag(res.copyPartResult().eTag())
                   .build();
           completedParts.add(part);
```

```
            partNum++;
            bytePosition += partSize;
        }
        return completedParts;
    }


    public static void multipartCopyUploadTest(S3Client s3, String srcBucket, String
 srcKey, String destnBucket, String destnKey)  {
        System.out.println("Starting multipart copy for: " + srcKey);
        try {
            String uploadId = createMultipartUpload(s3, destnBucket, destnKey);
            System.out.println(uploadId);
            ListCompletedPart parts = multipartUploadCopy(s3, srcBucket,
 srcKey,destnBucket,  destnKey, uploadId);
            completeMultipartUpload(s3, destnBucket, destnKey, uploadId, parts);
            System.out.println("Multipart copy completed for: " + srcKey);
        } catch (Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }
    }
```

SDK for Python

L'exemple suivant montre comment utiliser un chargement partitionné pour copier un objet par programmation d'un compartiment à un autre à l'aide du kit SDK pour Python.

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def head_object(s3_client, bucket_name, key_name):
    '''
    Returns metadata for an object in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains the object to query for metadata
    :param key_name: Key name to query for metadata
    :return: Metadata for the specified object if successful, else None
    '''
```

```
    try:
        response = s3_client.head_object(
            Bucket = bucket_name,
            Key = key_name
        )
        return response
    except ClientError as e:
        logging.error(e)
        return None

def create_multipart_upload(s3_client, bucket_name, key_name):
    '''
    Create a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :return: UploadId for the multipart upload if created successfully, else None
    '''

    try:
        mpu = s3_client.create_multipart_upload(Bucket = bucket_name, Key =
 key_name)
        return mpu['UploadId']
    except ClientError as e:
        logging.error(e)
        return None

def multipart_copy_upload(s3_client, source_bucket_name, key_name,
 target_bucket_name, mpu_id, part_size):
    '''
    Copy an object in a directory bucket to another bucket in multiple parts of a
 specified size

    :param s3_client: boto3 S3 client
    :param source_bucket_name: Bucket where the source object exists
    :param key_name: Key name of the object to be copied
    :param target_bucket_name: Destination bucket for copied object
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_size: The size parts that the object will be broken into, in bytes.
                      Minimum 5 MiB, Maximum 5 GiB. There is no minimum size for the
 last part of your multipart upload.
    :return: part_list for the multipart copy if all parts are copied successfully,
 else None
```

```
    '''

    part_list = []
    copy_source = {
        'Bucket': source_bucket_name,
        'Key': key_name
    }
    try:
        part_counter = 1
        object_size = head_object(s3_client, source_bucket_name, key_name)
        if object_size is not None:
            object_size = object_size['ContentLength']
        while (part_counter - 1) * part_size <object_size:
            bytes_start = (part_counter - 1) * part_size
            bytes_end = (part_counter * part_size) - 1
            upload_copy_part = s3_client.upload_part_copy (
                Bucket = target_bucket_name,
                CopySource = copy_source,
                CopySourceRange = f'bytes={bytes_start}-{bytes_end}',
                Key = key_name,
                PartNumber = part_counter,
                UploadId = mpu_id
            )
            part_list.append({'PartNumber': part_counter, 'ETag':
 upload_copy_part['CopyPartResult']['ETag']})
            part_counter += 1
    except ClientError as e:
        logging.error(e)
        return None
    return part_list

def complete_multipart_upload(s3_client, bucket_name, key_name, mpu_id, part_list):
    '''
    Completes a multipart upload to a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Destination bucket for the multipart upload
    :param key_name: Key name of the object to be uploaded
    :param mpu_id: The UploadId returned from the create_multipart_upload call
    :param part_list: List of uploaded part numbers with associated ETags
    :return: True if the multipart upload was completed successfully, else False
    '''

    try:
```

```
        s3_client.complete_multipart_upload(
            Bucket = bucket_name,
            Key = key_name,
            UploadId = mpu_id,
            MultipartUpload = {
                'Parts': part_list
            }
        )
    except ClientError as e:
        logging.error(e)
        return False
    return True

if __name__ == '__main__':
    MB = 1024 ** 2
    region = 'us-west-2'
    source_bucket_name = 'SOURCE_BUCKET_NAME'
    target_bucket_name = 'TARGET_BUCKET_NAME'
    key_name = 'KEY_NAME'
    part_size = 10 * MB
    s3_client = boto3.client('s3', region_name = region)
    mpu_id = create_multipart_upload(s3_client, target_bucket_name, key_name)
    if mpu_id is not None:
        part_list = multipart_copy_upload(s3_client, source_bucket_name, key_name,
 target_bucket_name, mpu_id, part_size)
        if part_list is not None:
            if complete_multipart_upload(s3_client, target_bucket_name, key_name,
 mpu_id, part_list):
                print (f'{key_name} successfully copied through multipart copy from
 {source_bucket_name} to {target_bucket_name}')
            else:
                print (f'Could not copy {key_name} through multipart copy from
 {source_bucket_name} to {target_bucket_name}')
```

À l'aide du AWS CLI

L'exemple suivant montre comment utiliser un chargement partitionné pour copier par programmation un objet d'un compartiment vers un compartiment de répertoire à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api upload-part-copy --bucket bucket-base-name--zone-id--x-s3 --
key TARGET_KEY_NAME --copy-source SOURCE_BUCKET_NAME/SOURCE_KEY_NAME --part-number 1 --
```

```
upload-id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

Pour de plus amples informations, veuillez consulter upload-part-copy dans le AWS Command Line Interface.

Affichage de la liste des chargements partitionnés en cours

Pour répertorier les téléchargements partitionnés en cours vers un bucket de répertoire, vous pouvez utiliser le AWS SDKs, ou le. AWS CLI

En utilisant le AWS SDKs

SDK for Java 2.x

Les exemples suivants montrent comment répertorier les chargements partitionnés (incomplets) en cours à l'aide du SDK pour Java 2.x.

Example

```
public static void listMultiPartUploads( S3Client s3, String bucketName) {
       try {
           ListMultipartUploadsRequest listMultipartUploadsRequest =
ListMultipartUploadsRequest.builder()
                .bucket(bucketName)
                .build();

           ListMultipartUploadsResponse response =
s3.listMultipartUploads(listMultipartUploadsRequest);
           List MultipartUpload uploads = response.uploads();
           for (MultipartUpload upload: uploads) {
               System.out.println("Upload in progress: Key = \"" + upload.key() +
"\", id = " + upload.uploadId());
           }
     }
     catch (S3Exception e) {
           System.err.println(e.getMessage());
           System.exit(1);
     }
 }
```

SDK for Python

Les exemples suivants montrent comment répertorier les chargements partitionnés (incomplets) en cours à l'aide du SDK pour Python.

Example

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_multipart_uploads(s3_client, bucket_name):
    '''
    List any incomplete multipart uploads in a directory bucket in e specified gion

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket to check for incomplete multipart uploads
    :return: List of incomplete multipart uploads if there are any, None if not
    '''

    try:
        response = s3_client.list_multipart_uploads(Bucket = bucket_name)
        if 'Uploads' in response.keys():
            return response['Uploads']
        else:
            return None
    except ClientError as e:
        logging.error(e)

if __name__ == '__main__':
    bucket_name = 'BUCKET_NAME'
    region = 'us-west-2'
    s3_client = boto3.client('s3', region_name = region)
    multipart_uploads = list_multipart_uploads(s3_client, bucket_name)
    if multipart_uploads is not None:
        print (f'There are {len(multipart_uploads)} ncomplete multipart uploads for
 {bucket_name}')
    else:
        print (f'There are no incomplete multipart uploads for {bucket_name}')
```

À l'aide du AWS CLI

Les exemples suivants montrent comment répertorier les chargements partitionnés (incomplets) en cours à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api list-multipart-uploads --bucket bucket-base-name--zone-id--x-s3
```

Pour de plus amples informations, veuillez consulter list-multipart-uploads dans le AWS Command Line Interface.

Affichage de la liste des parties d'un chargement partitionné

Les exemples suivants montrent comment répertorier les parties d'un chargement partitionné dans un compartiment de répertoires.

En utilisant le AWS SDKs

SDK for Java 2.x

Les exemples suivants montrent comment répertorier les parties d'un chargement partitionné dans un compartiment de répertoires à l'aide du kit SDK pour Java 2.x.

```
public static void listMultiPartUploadsParts( S3Client s3, String bucketName, String
 objKey, String uploadID) {

        try {
            ListPartsRequest listPartsRequest = ListPartsRequest.builder()
                .bucket(bucketName)
                .uploadId(uploadID)
                .key(objKey)
                .build();

            ListPartsResponse response = s3.listParts(listPartsRequest);
            ListPart parts = response.parts();
            for (Part part: parts) {
                System.out.println("Upload in progress: Part number = \"" +
 part.partNumber() + "\", etag = " + part.eTag());
            }

        }
```

```
        catch (S3Exception e) {
            System.err.println(e.getMessage());
            System.exit(1);
        }


    }
```

SDK for Python

Les exemples suivants montrent comment répertorier les parties d'un chargement partitionné dans un compartiment de répertoires à l'aide du kit SDK pour Python.

```
import logging
import boto3
from botocore.exceptions import ClientError

def list_parts(s3_client, bucket_name, key_name, upload_id):
    '''
    Lists the parts that have been uploaded for a specific multipart upload to a
 directory bucket.

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that multipart uploads parts have been uploaded to
    :param key_name: Name of the object that has parts uploaded
    :param upload_id: Multipart upload ID that the parts are associated with
    :return: List of parts associated with the specified multipart upload, None if
 there are no parts
    '''
    parts_list = []
    next_part_marker = ''
    continuation_flag = True
    try:
        while continuation_flag:
            if next_part_marker == '':
                response = s3_client.list_parts(
                    Bucket = bucket_name,
                    Key = key_name,
                    UploadId = upload_id
                )
            else:
                response = s3_client.list_parts(
                    Bucket = bucket_name,
```

```
                    Key = key_name,
                    UploadId = upload_id,
                    NextPartMarker = next_part_marker
                )
            if 'Parts' in response:
                for part in response['Parts']:
                    parts_list.append(part)
                if response['IsTruncated']:
                    next_part_marker = response['NextPartNumberMarker']
                else:
                    continuation_flag = False
            else:
                continuation_flag = False
        return parts_list
    except ClientError as e:
        logging.error(e)
        return None

if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    key_name = 'KEY_NAME'
    upload_id = 'UPLOAD_ID'
    s3_client = boto3.client('s3', region_name = region)
    parts_list = list_parts(s3_client, bucket_name, key_name, upload_id)
    if parts_list is not None:
        print (f'{key_name} has {len(parts_list)} parts uploaded to {bucket_name}')
    else:
        print (f'There are no multipart uploads with that upload ID for
 {bucket_name} bucket')
```

À l'aide du AWS CLI

Les exemples suivants montrent comment répertorier les parties d'un chargement partitionné dans un compartiment de répertoires à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3api list-parts --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME --upload-
id
 "AS_mgt9RaQE9GEaifATue15dAAAAAAAAAAEMAAAAAAAAADQwNzI4MDU0MjUyMBYAAAAAAAAAAA0AAAAAAAAAAH2AfYAA
```

Pour plus d'informations, consultez list-parts dans l' AWS Command Line Interface.

Copie d'objets vers ou depuis un compartiment de répertoires

L'opération de copie crée une copie d'un objet déjà stocké dans Amazon S3. Vous pouvez copier des objets entre des compartiments de répertoires et des compartiments à usage général. Vous pouvez également copier des objets au sein d'un compartiment et entre des compartiments du même type, par exemple, d'un compartiment de répertoires à un autre.

> **Note**
>
> La copie d'objets entre différents Régions AWS n'est pas prise en charge lorsque le compartiment source ou de destination se trouve dans une zone AWS locale. Les compartiments source et de destination doivent avoir la même Région AWS parent. Les compartiments source et de destination peuvent correspondre à différents types d'emplacement de compartiment (zone de disponibilité ou zone locale).

Vous pouvez créer une copie d'un objet d'une taille maximale de 5 Go dans une seule opération atomique. Toutefois, pour copier un objet supérieur à 5 Go, vous devez utiliser les opérations d'API de chargement partitionné. Pour de plus amples informations, veuillez consulter Utilisation du chargement partitionné avec les compartiments de répertoires.

Autorisations

Pour copier des objets, vous devez disposer des autorisations suivantes :

- Pour copier des objets d'un compartiment de répertoires vers un autre, vous devez disposer de l'autorisation `s3express:CreateSession`.
- Pour copier des objets à partir de compartiments de répertoires vers des compartiments à usage général, vous devez disposer de l'autorisation `s3express:CreateSession` et de l'autorisation `s3:PutObject` permettant d'écrire la copie des objets dans le compartiment de destination.
- Pour copier des objets à partir de compartiments à usage général vers des compartiments de répertoires, vous devez disposer de l'autorisation `s3express:CreateSession` et de l'autorisation `s3:GetObject` permettant de lire l'objet source à copier.

  Pour plus d'informations, consultez CopyObject dans la Référence d'API Amazon Simple Storage Service.

Chiffrement

Amazon S3 chiffre automatiquement tous les nouveaux objets chargés dans un compartiment S3. La configuration de chiffrement par défaut d'un compartiment S3 est toujours activée et est au minimum définie sur le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3).

Pour les compartiments d'annuaire, le SSE-S3 et le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) sont pris en charge. Lorsque le compartiment de destination est un compartiment de répertoires, nous recommandons que le chiffrement par défaut du compartiment de destination utilise la configuration de chiffrement souhaitée et que vous ne remplaciez pas le chiffrement par défaut du compartiment. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. De plus, les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de l'opération CopyObject. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS. Pour plus d'informations sur les comportements de remplacement du chiffrement dans les compartiments de répertoire, voir Spécifier le chiffrement côté serveur avec AWS KMS pour les téléchargements de nouveaux objets.

Pour les compartiments à usage général, vous pouvez utiliser le SSE-S3 (par défaut), le chiffrement côté serveur avec des clés () AWS Key Management Service (SSE-KMS AWS KMS), le chiffrement double couche côté serveur avec des clés (DSSE-KMS) ou le chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C).

Si vous effectuez une demande de copie qui indique d'utiliser le chiffrement DSSE-KMS ou SSE-C pour un compartiment de répertoires (compartiment source ou cible), la réponse renverra une erreur.

Balises

Les compartiments de répertoires ne prennent pas en charge les balises. Si vous copiez un objet contenant des balises à partir d'un compartiment à usage général vers un compartiment de répertoires, vous recevez une réponse HTTP `501 (Not Implemented)`. Pour plus d'informations, consultez CopyObject dans la Référence d'API Amazon Simple Storage Service.

ETags

Les balises d'entité (ETags) pour S3 Express One Zone sont des chaînes alphanumériques aléatoires et ne sont pas des MD5 checksums. Pour garantir l'intégrité des objets, utilisez des sommes de contrôle supplémentaires.

Sommes de contrôle supplémentaires

S3 Express One Zone vous offre la possibilité de choisir l'algorithme de somme de contrôle utilisé pour valider vos données pendant le chargement ou le téléchargement. Vous pouvez sélectionner l'un des algorithmes de hachage sécurisé (SHA) ou de contrôle de redondance cyclique (CRC) suivants : CRC32 C CRC32, SHA-1 et SHA-256. MD5les checksums basés sur la base de données ne sont pas pris en charge avec la classe de stockage S3 Express One Zone.

Pour de plus amples informations, veuillez consulter Bonnes pratiques supplémentaires en matière de somme de contrôle S3.

Fonctionnalités prises en charge

Pour plus d'informations sur les fonctionnalités Amazon S3 prises en charge pour S3 Express One Zone, consultez Différences pour les compartiments de répertoires.

Utilisation de la console S3 (copie vers un compartiment de répertoires)

> **Note**
>
> Voici les restrictions et limites qui s'appliquent lorsque vous copiez un objet dans un compartiment de répertoires avec la console :
>
> - L'action Copy s'applique à tous les objets des dossiers spécifiés (préfixes). Les objets ajoutés à ces dossiers pendant que l'action est en cours risquent d'être affectés.
> - Les objets chiffrés avec des clés de chiffrement fournies par le client (SSE-C) ne peuvent pas être copiés à l'aide de la console S3. Pour copier des objets chiffrés avec SSE-C, utilisez le AWS CLI AWS SDK ou l'API REST Amazon S3.
> - Les objets copiés ne conservent pas les paramètres de verrouillage des objets d'origine.
> - Si le compartiment à partir duquel vous copiez des objets utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, l'objet ne ACLs sera pas copié vers la destination spécifiée.
> - Si vous souhaitez copier des objets dans un compartiment qui utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, assurez-vous que le compartiment source utilise également le paramètre imposé par le propriétaire du compartiment, ou supprimez tout objet accordé par l'ACL à d'autres AWS comptes et groupes.
> - Les objets copiés d'un compartiment à usage général vers un compartiment de répertoire ne conserveront pas les balises d'objet ni les valeurs Etag. ACLs Les valeurs de somme

de contrôle peuvent être copiées, mais ne sont pas équivalentes à une balise d'entité. La valeur d'une somme de contrôle peut changer par rapport au moment où elle a été ajoutée.

- Tous les objets copiés dans un compartiment de répertoires présentent le paramètre Propriétaire du compartiment appliqué pour la propriété des objets S3.

Pour copier un objet d'un compartiment à usage général vers un compartiment de répertoires

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, le type de compartiment à partir duquel vous souhaitez copier des objets :

   - Pour copier des objets à partir d'un compartiment à usage général, choisissez l'onglet Compartiments à usage général.
   - Pour copier des objets à partir d'un compartiment de répertoires, choisissez l'onglet Compartiments de répertoires.
3. Choisissez le compartiment à usage général ou le compartiment de répertoires contenant les objets que vous souhaitez copier.
4. Cliquez sur l'onglet Objets. Sur la page Objets, cochez la case située à gauche du nom des objets que vous souhaitez copier.
5. Dans le menu Actions, choisissez Copier.

   La page Copier s'affiche.
6. Sous Destination, choisissez Compartiment de répertoires pour votre type de destination. Pour spécifier le chemin de destination, choisissez Parcourir S3, accédez à la destination, puis cochez la case située à gauche de la destination. Choisissez Choose destination (Choisir une destination) en bas à droite.

   Vous pouvez également saisir le chemin de destination.
7. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécification des paramètres pour définir les paramètres du chiffrement côté serveur, des sommes de contrôle et des métadonnées.

8. En bas à droite, choisissez Copy (Copier). Amazon S3 copie votre objet dans la destination.

Utilisation de la console S3 (copie vers un compartiment à usage général)

> **Note**
>
> Voici les restrictions et limites qui s'appliquent lorsque vous copiez un objet dans un compartiment à usage général avec la console :
>
> - L'action Copy s'applique à tous les objets des dossiers spécifiés (préfixes). Les objets ajoutés à ces dossiers pendant que l'action est en cours risquent d'être affectés.
> - Les objets chiffrés avec des clés de chiffrement fournies par le client (SSE-C) ne peuvent pas être copiés à l'aide de la console S3. Pour copier des objets chiffrés avec SSE-C, utilisez le AWS CLI AWS SDK ou l'API REST Amazon S3.
> - Les objets copiés ne conservent pas les paramètres de verrouillage des objets d'origine.
> - Si le compartiment à partir duquel vous copiez des objets utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, l'objet ne ACLs sera pas copié vers la destination spécifiée.
> - Si vous souhaitez copier des objets dans un compartiment qui utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, assurez-vous que le compartiment source utilise également le paramètre imposé par le propriétaire du compartiment, ou supprimez tout objet accordé par l'ACL à d'autres AWS comptes et groupes.

Pour copier un objet d'un compartiment de répertoires vers un compartiment à usage général

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Choisissez l'onglet Compartiments de répertoires.
4. Choisissez le compartiment de répertoires contenant les objets que vous souhaitez copier.
5. Cliquez sur l'onglet Objets. Sur la page Objets, cochez la case située à gauche du nom des objets que vous souhaitez copier.
6. Dans le menu Actions, choisissez Copier.

7. Sous Destination, choisissez Compartiment à usage général pour votre type de destination. Pour spécifier le chemin de destination, choisissez Parcourir S3, accédez à la destination, puis cochez la case située à gauche de la destination. Choisissez Choose destination (Choisir une destination) en bas à droite.

   Vous pouvez également saisir le chemin de destination.

8. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.
9. En bas à droite, choisissez Copy (Copier). Amazon S3 copie votre objet dans la destination.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

```
public static void copyBucketObject (S3Client s3, String sourceBucket, String
objectKey, String targetBucket) {
     CopyObjectRequest copyReq = CopyObjectRequest.builder()
         .sourceBucket(sourceBucket)
         .sourceKey(objectKey)
         .destinationBucket(targetBucket)
         .destinationKey(objectKey)
         .build();
      String temp = "";

      try {
          CopyObjectResponse copyRes = s3.copyObject(copyReq);
          System.out.println("Successfully copied " + objectKey +" from bucket " +
sourceBucket +" into bucket "+targetBucket);
      }

      catch (S3Exception e) {
          System.err.println(e.awsErrorDetails().errorMessage());
          System.exit(1);
```

```
        }
}
```

À l'aide du AWS CLI

L'`copy-object`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour copier un objet d'un compartiment vers un autre. Vous pouvez copier des objets d'un type de compartiment à l'autre. Pour exécuter cette commande, remplacez les espaces réservés d'entrée utilisateur par vos propres informations.

```
aws s3api copy-object --copy-source SOURCE_BUCKET/SOURCE_KEY_NAME --key TARGET_KEY_NAME
 --bucket TARGET_BUCKET_NAME
```

Pour plus d'informations, consultez copy-object dans la Référence des commandes de l'AWS CLI .

Suppression d'objets à partir d'un compartiment de répertoires

Vous pouvez supprimer des objets d'un compartiment d'annuaire Amazon S3 à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) ou AWS SDKs. Pour plus d'informations, consultez Utilisation des compartiments de répertoires et S3 Express One Zone.

Warning

- La suppression d'un objet est irréversible.
- Cette action supprime tous les objets spécifiés. Lorsque vous supprimez des dossiers, attendez la fin de l'action de suppression pour ajouter de nouveaux objets au dossier. Dans le cas contraire, de nouveaux objets pourraient également être supprimés.

Note

Lorsque vous supprimez plusieurs objets d'un compartiment de répertoires par programmation, notez les points suivants :

- Les clés d'objet figurant dans les demandes `DeleteObjects` doivent contenir au moins un caractère autre qu'une espace. Les chaînes composées uniquement d'espaces ne sont pas prises en charge.

- Les clés d'objet figurant dans les demandes `DeleteObjects` ne peuvent pas contenir de caractères de contrôle Unicode, à l'exception des sauts de ligne (`\n`), des tabulations (`\t`) et des retour chariot (`\r`).

Utilisation de la console S3

Pour supprimer des objets

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Directory buckets.
3. Choisissez le compartiment de répertoires contenant les objets que vous souhaitez supprimer.
4. Cliquez sur l'onglet Objets. Dans la liste Objets, cochez la case en regard des objets que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer).
6. Sur la page Supprimer des objets, entrez **`permanently delete`** dans la zone de texte.
7. Choisissez Supprimer les objets.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

L'exemple suivant illustre la suppression d'objets dans un compartiment de répertoires à l'aide du kit AWS SDK for Java 2.x.

```
static void deleteObject(S3Client s3Client, String bucketName, String objectKey) {



       try {

           DeleteObjectRequest del = DeleteObjectRequest.builder()
                   .bucket(bucketName)
                   .key(objectKey)
                   .build();
```

```
            s3Client.deleteObject(del);

            System.out.println("Object " + objectKey + " has been deleted");


        } catch (S3Exception e) {
            System.err.println(e.awsErrorDetails().errorMessage());
            System.exit(1);
        }

    }
```

SDK for Python

Example

L'exemple suivant illustre la suppression d'objets dans un compartiment de répertoires à l'aide du kit AWS SDK pour Python (Boto3).

```
import logging
import boto3
from botocore.exceptions import ClientError

def delete_objects(s3_client, bucket_name, objects):
    '''
    Delete a list of objects in a directory bucket

    :param s3_client: boto3 S3 client
    :param bucket_name: Bucket that contains objects to be deleted; for example,
 'doc-example-bucket--usw2-az1--x-s3'
    :param objects: List of dictionaries that specify the key names to delete
    :return: Response output, else False
    '''

    try:
        response = s3_client.delete_objects(
            Bucket = bucket_name,
            Delete = {
                'Objects': objects
            }
        )
        return response
```

```
    except ClientError as e:
        logging.error(e)
        return False


if __name__ == '__main__':
    region = 'us-west-2'
    bucket_name = 'BUCKET_NAME'
    objects = [
        {
            'Key': '0.txt'
        },
        {
            'Key': '1.txt'
        },
        {
            'Key': '2.txt'
        },
        {
            'Key': '3.txt'
        },
        {
            'Key': '4.txt'
        }
    ]

    s3_client = boto3.client('s3', region_name = region)
    results = delete_objects(s3_client, bucket_name, objects)
    if results is not None:
        if 'Deleted' in results:
            print (f'Deleted {len(results["Deleted"])} objects from {bucket_name}')
        if 'Errors' in results:
            print (f'Failed to delete {len(results["Errors"])} objects from
 {bucket_name}')
```

À l'aide du AWS CLI

L'exemple de commande `delete-object` suivant illustre la façon d'utiliser l' AWS CLI pour supprimer un objet d'un compartiment de répertoires. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api delete-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

Pour plus d'informations, consultez delete-object dans la Référence des commandes de l'AWS CLI .

L'`delete-objects`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour supprimer des objets d'un compartiment de répertoire. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

Le `delete.json` fichier est le suivant :

```
{
    "Objects": [
        {
            "Key": "0.txt"
        },
        {
            "Key": "1.txt"
        },
        {
            "Key": "2.txt"
        },
        {
            "Key": "3.txt"
        }
    ]
}
```

L'`delete-objects`exemple de commande est le suivant :

```
aws s3api delete-objects --bucket bucket-base-name--zone-id--x-s3 --delete
 file://delete.json
```

Pour plus d'informations, consultez delete-objects dans la Référence des commandes de l'AWS CLI .

Téléchargement d'un objet à partir d'un compartiment de répertoires

Les exemples de code suivants montrent comment lire (télécharger) les données d'un objet dans un compartiment de répertoires Amazon S3 à l'aide de l'opération d'API `GetObject`.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

Les exemples de code suivants montrent comment lire les données à partir d'un objet dans un compartiment de répertoires à l'aide du kit AWS SDK for Java 2.x.

```
public static void getObject(S3Client s3Client, String bucketName, String objectKey)
 {
     try {
         GetObjectRequest objectRequest = GetObjectRequest
            .builder()
            .key(objectKey)
            .bucket(bucketName)
            .build();

         ResponseBytes GetObjectResponse objectBytes =
 s3Client.getObjectAsBytes(objectRequest);
         byte[] data = objectBytes.asByteArray();

         //Print object contents to console
         String s = new String(data, StandardCharsets.UTF_8);
         System.out.println(s);
    }

    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
        System.exit(1);
    }
}
```

SDK for Python

Example

Les exemples de code suivants montrent comment lire les données à partir d'un objet dans un compartiment de répertoires à l'aide du kit AWS SDK pour Python (Boto3).

```
import boto3
from botocore.exceptions import ClientError
```

```
from botocore.response import StreamingBody

def get_object(s3_client: boto3.client, bucket_name: str, key_name: str) ->
 StreamingBody:
    """
    Gets the object.
    :param s3_client:
    :param bucket_name: The bucket that contains the object.
    :param key_name: The key of the object to be downloaded.
    :return: The object data in bytes.
    """
    try:
        response = s3_client.get_object(Bucket=bucket_name, Key=key_name)
        body = response['Body'].read()
        print(f"Got object '{key_name}' from bucket '{bucket_name}'.")
    except ClientError:
        print(f"Couldn't get object '{key_name}' from bucket '{bucket_name}'.")
        raise
    else:
        return body

def main():
    s3_client = boto3.client('s3')
    resp = get_object(s3_client, 'doc-example-bucket--use1-az4--x-s3', 'sample.txt')
    print(resp)

if __name__ == "__main__":
     main()
```

À l'aide du AWS CLI

L'exemple de commande `get-object` suivant montre comment utiliser l'interface AWS CLI pour télécharger un objet depuis Amazon S3. Cette commande récupère l'objet *KEY_NAME* à partir du compartiment de répertoires *bucket-base-name*`--`*zone-id*`--x-s3`. L'objet sera téléchargé dans un fichier nommé *LOCAL_FILE_NAME*. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3api get-object --bucket bucket-base-name--zone-id--x-s3 --
key KEY_NAME LOCAL_FILE_NAME
```

Pour plus d'informations, consultez get-object dans la Référence des commandes de l'AWS CLI .

Génération d'un bucket URLs de répertoire présigné pour partager des objets

Les exemples de code suivants montrent comment générer des objets présignés URLs pour partager à partir d'un compartiment d'annuaire Amazon S3.

À l'aide du AWS CLI

L'exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour générer une URL présignée pour un objet depuis Amazon S3. Cette commande génère une URL présignée pour un objet *KEY_NAME* à partir du compartiment *bucket-base-name*--*zone-id*--x-s3 de répertoire. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3 presign s3://bucket-base-name--zone-id--x-s3/KEY_NAME --expires-in 7200
```

Pour plus d'informations, consultez presign dans la Référence des commandes de l'AWS CLI .

Récupération des métadonnées d'objets à partir de compartiments de répertoires

Les exemples de AWS SDK et de AWS CLI suivants montrent comment utiliser l'opération `HeadObject` et l'`GetObjectAttributes`API pour récupérer les métadonnées d'un objet dans un compartiment d'annuaire Amazon S3 sans renvoyer l'objet lui-même.

En utilisant le AWS SDKs

SDK for Java 2.x

Example

```
public static void headObject(S3Client s3Client, String bucketName, String
 objectKey) {
     try {
         HeadObjectRequest headObjectRequest = HeadObjectRequest
                 .builder()
                 .bucket(bucketName)
                 .key(objectKey)
```

```
                .build();
        HeadObjectResponse response = s3Client.headObject(headObjectRequest);
        System.out.format("Amazon S3 object: \"%s\" found in bucket: \"%s\" with
ETag: \"%s\"", objectKey, bucketName, response.eTag());
    }
    catch (S3Exception e) {
        System.err.println(e.awsErrorDetails().errorMessage());
```

À l'aide du AWS CLI

L'`head-object`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour récupérer les métadonnées d'un objet. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api head-object --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
```

Pour plus d'informations, consultez head-object dans la Référence des commandes de l'AWS CLI .

L'`get-object-attributes`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour récupérer les métadonnées d'un objet. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api get-object-attributes --bucket bucket-base-name--zone-id--x-s3 --key KEY_NAME
 --object-attributes "StorageClass" "ETag" "ObjectSize"
```

Pour plus d'informations, consultez get-object-attributes dans la Référence des commandes de l'AWS CLI .

Répertorier les objets d'un bucket de répertoire

Les exemples de code suivants montrent comment répertorier des objets dans un bucket d'annuaire Amazon S3 à l'aide de l'opération `ListObjectsV2` API.

À l'aide du AWS CLI

L'`list-objects-v2`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour répertorier des objets depuis Amazon S3. Cette commande répertorie les objets du bucket du répertoire*`bucket-base-name`*`--`*`zone-id`*`--x-s3`. Pour exécuter cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api list-objects-v2 --bucket bucket-base-name--zone-id--x-s3
```

Pour plus d'informations, consultez list-objects-v2 dans la Référence des commandes de l'AWS CLI .

Sécurité des compartiments de répertoires

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures 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 chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des AWS Compliance Programs.

  Pour en savoir plus sur les programmes de conformité, consultez Services AWS in Scope by Compliance Program.
- Sécurité dans le cloud — Votre responsabilité est déterminée par Service AWS ce que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris la sensibilité de vos données, les exigences de votre entreprise, et la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de compartiments de répertoires. Les rubriques suivantes expliquent comment configurer les compartiments de répertoires pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à en utiliser d'autres Services AWS qui peuvent vous aider à surveiller et à sécuriser vos objets dans des compartiments de répertoires.

Protection et chiffrement des données

Pour plus d'informations sur la façon de configurer le chiffrement des compartiments de répertoires, consultez les rubriques suivantes.

Rubriques

- Chiffrement côté serveur

- Configuration et surveillance du chiffrement par défaut pour les compartiments de répertoires
- Utilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de répertoire
- Chiffrement en transit
- Suppression de données

Chiffrement côté serveur

Le chiffrement est configuré par défaut pour tous les compartiments de répertoires, et tous les nouveaux objets qui sont chargés dans les compartiments de répertoires sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment de répertoires. Si vous souhaitez spécifier un autre type de chiffrement, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), en définissant la configuration de chiffrement par défaut du compartiment. Pour plus d'informations sur le chiffrement SSE-KMS dans les compartiments de répertoires, consultez Utilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de répertoire.

Nous recommandons que le chiffrement par défaut du compartiment utilise la configuration de chiffrement souhaitée et que vous ne remplaciez pas le chiffrement par défaut du compartiment dans vos demandes `CreateSession` ni dans vos demandes d'objets PUT. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. Pour plus d'informations sur les comportements de remplacement du chiffrement dans les compartiments de répertoire, voir Spécifier le chiffrement côté serveur avec AWS KMS pour les téléchargements de nouveaux objets.

Le chiffrement SSE-KMS avec les compartiments de répertoires diffère du chiffrement SSE-KMS dans les compartiments à usage général sur les points suivants.

- Votre configuration SSE-KMS ne peut prendre en charge qu'une seule clé gérée par le client par compartiment de répertoires pendant toute la durée de vie du compartiment. La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. De même, après avoir spécifié une clé gérée par le client pour SSE-KMS, vous ne pouvez pas remplacer la clé gérée par le client pour la configuration SSE-KMS du compartiment.

  Vous pouvez identifier la clé gérée par le client que vous avez spécifiée pour la configuration SSE-KMS du compartiment de la manière suivante :

- Effectuez une demande d'opération d'API `HeadObject` pour trouver la valeur de `x-amz-server-side-encryption-aws-kms-key-id` dans la réponse.

Pour utiliser une nouvelle clé gérée par le client pour vos données, nous vous recommandons de copier vos objets existants dans un nouveau compartiment de répertoires avec une nouvelle clé gérée par le client.

- Pour les opérations d'API du point de terminaison zonal (au niveau de l'objet), à l'exception de CopyObjectet UploadPartCopy, vous authentifiez et autorisez les demandes pour une faible latence. CreateSession Nous recommandons que le chiffrement par défaut du compartiment utilise la configuration de chiffrement souhaitée et que vous ne remplaciez pas le chiffrement par défaut du compartiment dans vos demandes `CreateSession` ni dans vos demandes d'objets PUT. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. Pour chiffrer de nouveaux objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). Ensuite, lorsqu'une session sera créée pour les opérations de l'API de point de terminaison zonal, les nouveaux objets seront automatiquement chiffrés et déchiffrés avec les clés SSE-KMS et les clés de compartiment S3 pendant la session. Pour plus d'informations sur les comportements de remplacement du chiffrement dans les compartiments de répertoire, voir Spécifier le chiffrement côté serveur avec AWS KMS pour les téléchargements de nouveaux objets.

  Dans les appels d'API du point de terminaison zonal (sauf CopyObjectet UploadPartCopy), vous ne pouvez pas remplacer les valeurs des paramètres de chiffrement (`x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-idx-amz-server-side-encryption-context`, et`x-amz-server-side-encryption-bucket-key-enabled`) de la `CreateSession` demande. Il n'est pas nécessaire de spécifier explicitement les valeurs de ces paramètres de chiffrement dans les appels d'API de point de terminaison zonal. Amazon S3 utilisera les valeurs des paramètres de chiffrement de la demande `CreateSession` pour protéger les nouveaux objets dans le compartiment de répertoires.

  > **Note**
  >
  > Lorsque vous utilisez le AWS CLI ou le AWS SDKs, pour`CreateSession`, le jeton de session est automatiquement actualisé pour éviter les interruptions de service à l'expiration d'une session. AWS CLI Ou AWS SDKs utilisez la configuration de chiffrement par défaut du compartiment pour la `CreateSession` demande. Il n'est pas possible de remplacer les valeurs des paramètres de chiffrement dans la demande `CreateSession`. De plus,

dans les appels d'API du point de terminaison zonal (sauf CopyObjectet UploadPartCopy), il n'est pas possible de remplacer les valeurs des paramètres de chiffrement de la `CreateSession` demande.

- En effet CopyObject, pour chiffrer de nouvelles copies d'objets dans un compartiment d'annuaire avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut du compartiment d'annuaire avec une clé KMS (en particulier, une clé gérée par le client). Ensuite, lorsque vous spécifierez les paramètres de chiffrement côté serveur pour les nouvelles copies d'objets avec SSE-KMS, vous devrez vous assurer que la clé de chiffrement est la clé gérée par le client que vous avez spécifiée pour la configuration de chiffrement par défaut du compartiment de répertoires. En effet UploadPartCopy, pour chiffrer de nouvelles copies partielles d'objets dans un compartiment d'annuaire avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut du compartiment d'annuaire avec une clé KMS (en particulier, une clé gérée par le client). Vous ne pouvez pas spécifier de paramètres de chiffrement côté serveur pour les nouvelles copies partielles d'objets avec SSE-KMS dans les en-têtes de demande. UploadPartCopy En outre, les paramètres de chiffrement que vous fournissez dans la CreateMultipartUploaddemande doivent correspondre à la configuration de chiffrement par défaut du compartiment de destination.
- Les clés de compartiment S3 sont toujours activées pour les opérations `GET` et `PUT` dans un compartiment de répertoires et ne peuvent pas être désactivées. Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de CopyObject, d'UploadPartCopy, de l'opération Copy dans les opérations par lot ou des tâches import. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS.
- Lorsque vous spécifiez une cléAWS KMS gérée par le client pour le chiffrement dans votre compartiment de répertoires, utilisez uniquement l'ID ou l'ARN de la clé. Le format de l'alias de la clé KMS n'est pas pris en charge.

Les compartiments d'annuaire ne prennent pas en charge le chiffrement double couche côté serveur avec des clés AWS Key Management Service (AWS KMS) (DSSE-KMS), ni le chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C).

Configuration et surveillance du chiffrement par défaut pour les compartiments de répertoires

Les compartiments Amazon S3 ont le chiffrement des compartiments activé par défaut et les nouveaux objets sont automatiquement chiffrés à l'aide du chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3). Ce chiffrement s'applique à tous les nouveaux objets de vos compartiments Amazon S3, sans frais.

Si vous avez besoin d'un contrôle accru sur vos clés de chiffrement, par exemple pour gérer la rotation des clés et l'attribution des politiques d'accès, vous pouvez choisir d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS).

> **Note**
>
> - Nous recommandons que le chiffrement par défaut du compartiment utilise la configuration de chiffrement souhaitée et que vous ne remplaciez pas le chiffrement par défaut du compartiment dans vos demandes `CreateSession` ni dans vos demandes d'objets PUT. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. Pour plus d'informations sur les comportements de remplacement du chiffrement dans les compartiments de répertoire, voir Spécifier le chiffrement côté serveur avec AWS KMS pour les téléchargements de nouveaux objets.
> - Pour chiffrer de nouveaux objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). Ensuite, lorsqu'une session sera créée pour les opérations de l'API de point de terminaison zonal, les nouveaux objets seront automatiquement chiffrés et déchiffrés avec les clés SSE-KMS et les clés de compartiment S3 pendant la session.
> - Lorsque vous définissez le chiffrement SSE-KMS par défaut pour les compartiments, les clés de compartiment S3 sont toujours activées pour les opérations `GET` et PUT dans un compartiment de répertoires et ne peuvent pas être désactivées. Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de CopyObject, d'UploadPartCopy, de l'opération Copy dans les opérations par lot ou des tâches import. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS. Pour plus d'informations sur la façon dont les clés de compartiment S3 réduisent

les coûts de vos AWS KMS demandes, consultezRéduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

- Lorsque vous spécifiez une cléAWS KMS gérée par le client pour le chiffrement dans votre compartiment de répertoires, utilisez uniquement l'ID ou l'ARN de la clé. Le format de l'alias de la clé KMS n'est pas pris en charge.
- Le chiffrement double couche côté serveur avec AWS KMS clés (DSSE-KMS) et le chiffrement côté serveur avec clés fournies par le client (SSE-C) ne sont pas pris en charge pour le chiffrement par défaut dans les compartiments d'annuaire.

Pour plus d'informations sur la configuration du chiffrement par défaut, consultez Configuration du chiffrement par défaut.

Pour en savoir plus sur les autorisations nécessaires pour le chiffrement par défaut, consultez PutBucketEncryption dans la documentation de référence de l'API Amazon Simple Storage Service.

Vous pouvez configurer le chiffrement par défaut d'Amazon S3 pour un compartiment S3 à l'aide de la console Amazon S3 AWS SDKs, de l'API REST Amazon S3 et du AWS Command Line Interface (AWS CLI).

Utilisation de la console S3

Pour configurer le chiffrement par défaut sur un compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment que vous souhaitez utiliser.
4. Choisissez l'onglet Propriétés.
5. Dans Paramètres de chiffrement côté serveur, les compartiments de répertoires utilisent le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).
6. Sélectionnez Enregistrer les modifications.

À l'aide du AWS CLI

Ces exemples montrent comment configurer le chiffrement par défaut en utilisant SSE-S3 ou SSE-KMS avec une clé de compartiment S3.

Pour plus d'informations sur le chiffrement par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Pour plus d'informations sur l'utilisation du AWS CLI pour configurer le chiffrement par défaut, consultez put-bucket-encryption.

Example — Chiffrement par défaut avec SSE-S3

Cet exemple montre comment configurer le chiffrement du compartiment par défaut avec les clés gérées par Amazon S3. Pour utiliser la commande, remplacez-la *user input placeholders* par vos propres informations.

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-
encryption-configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            }
        }
    ]
}'
```

Example — Chiffrement par défaut avec SSE-KMS à l'aide d'une clé de compartiment S3

Cet exemple configure le chiffrement du compartiment par défaut avec SSE-KMS à l'aide d'une clé de compartiment S3. Pour utiliser la commande, remplacez-la *user input placeholders* par vos propres informations.

```
aws s3api put-bucket-encryption --bucket bucket-base-name--zone-id--x-s3 --server-side-
encryption-configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
```

```
        ]
    }'
```

Utilisation de l'API REST

Utilisez l'opération `PutBucketEncryption` de l'API REST pour définir le chiffrement par défaut avec un type de chiffrement côté serveur à utiliser : SSE-S3 ou SSE-KMS.

Pour plus d'informations, consultez PutBucketEncryption dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Lors de l'utilisation AWS SDKs, vous pouvez demander à Amazon S3 de l'utiliser AWS KMS keys pour le chiffrement côté serveur. Les exemples suivants AWS SDKs pour Java et .NET configurent la configuration de chiffrement par défaut pour un compartiment de répertoire avec SSE-KMS et une clé de compartiment S3. Pour plus d'informations sur les autres SDKs, consultez la section Exemples de code et de bibliothèques sur le AWS Developer Center.

> **Important**
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 ne prend en charge que les clés KMS à chiffrement symétrique. Pour plus d'informations sur ces clés, consultez Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

Java

Avec le AWS SDK for Java 2.x, vous pouvez demander à Amazon S3 d'utiliser un AWS KMS key en utilisant la `applyServerSideEncryptionByDefault` méthode pour spécifier la configuration de chiffrement par défaut de votre compartiment d'annuaire pour le chiffrement des données avec SSE-KMS. Vous créez une clé KMS symétrique de chiffrement et la spécifier dans la demande.

```
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.PutBucketEncryptionRequest;
import software.amazon.awssdk.services.s3.model.ServerSideEncryption;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionByDefault;
```

```
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionConfiguration;
import software.amazon.awssdk.services.s3.model.ServerSideEncryptionRule;

public class Main {
    public static void main(String[] args) {
        S3Client s3 = S3Client.create();
        String bucketName = "bucket-base-name--zoneid--x-s3";
        String kmsKeyId = "your-kms-customer-managed-key-id";

        // AWS managed KMS keys aren't supported. Only customer-managed keys are
 supported.
        ServerSideEncryptionByDefault serverSideEncryptionByDefault =
 ServerSideEncryptionByDefault.builder()
                .sseAlgorithm(ServerSideEncryption.AWS_KMS)
                .kmsMasterKeyID(kmsKeyId)
                .build();

        // The bucketKeyEnabled field is enforced to be true.
        ServerSideEncryptionRule rule = ServerSideEncryptionRule.builder()
                .bucketKeyEnabled(true)
                .applyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
                .build();

        ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
 ServerSideEncryptionConfiguration.builder()
                .rules(rule)
                .build();

        PutBucketEncryptionRequest putRequest = PutBucketEncryptionRequest.builder()
                .bucket(bucketName)

 .serverSideEncryptionConfiguration(serverSideEncryptionConfiguration)
                .build();

        s3.putBucketEncryption(putRequest);

    }
}
```

Pour plus d'informations sur la création de clés gérées par le client, consultez la section Programmation de l' AWS KMS API dans le Guide du AWS Key Management Service développeur.

Pour obtenir des exemples de code utilisables pour charger un objet, consultez les rubriques suivantes. Pour utiliser ces exemples, vous devez mettre à jour les exemples de code et fournir des informations de chiffrement comme illustré dans le fragment de code précédent.

- Pour charger un objet en une seule opération, consultez Chargement d'objets dans un compartiment de répertoires.
- Pour les opérations d'API de chargement partitionné, consultez Utilisation du chargement partitionné avec les compartiments de répertoires.

.NET

Avec le AWS SDK pour .NET, vous pouvez demander à Amazon S3 d'utiliser un AWS KMS key en utilisant la `ServerSideEncryptionByDefault` propriété pour spécifier la configuration de chiffrement par défaut de votre compartiment d'annuaire pour le chiffrement des données avec SSE-KMS. Vous créez une clé symétrique de chiffrement gérée par le client et la spécifier dans la demande.

```
    // Set the bucket server side encryption to use AWSKMS with a customer-managed
 key id.
    // bucketName: Name of the directory bucket. "bucket-base-name--zonsid--x-s3"
    // kmsKeyId: The Id of the customer managed KMS Key. "your-kms-customer-managed-
key-id"
    // Returns True if successful.
    public static async Task<bool> SetBucketServerSideEncryption(string bucketName,
 string kmsKeyId)
    {
        var serverSideEncryptionByDefault = new ServerSideEncryptionConfiguration
        {
            ServerSideEncryptionRules = new List<ServerSideEncryptionRule>
            {
                new ServerSideEncryptionRule
                {
                    ServerSideEncryptionByDefault = new
 ServerSideEncryptionByDefault
                    {
```

```
                        ServerSideEncryptionAlgorithm =
ServerSideEncryptionMethod.AWSKMS,
                        ServerSideEncryptionKeyManagementServiceKeyId = kmsKeyId
                    }
                }
            }
        };
        try
        {
            var encryptionResponse =await _s3Client.PutBucketEncryptionAsync(new
PutBucketEncryptionRequest
            {
                BucketName = bucketName,
                ServerSideEncryptionConfiguration = serverSideEncryptionByDefault,
            });

            return encryptionResponse.HttpStatusCode == HttpStatusCode.OK;
        }
        catch (AmazonS3Exception ex)
        {
            Console.WriteLine(ex.ErrorCode == "AccessDenied"
                ? $"This account does not have permission to set encryption on
{bucketName}, please try again."
                : $"Unable to set bucket encryption for bucket {bucketName},
{ex.Message}");
        }
        return false;
    }
```

Pour plus d'informations sur la création de clés gérées par le client, consultez la section Programmation de l' AWS KMS API dans le Guide du AWS Key Management Service développeur.

Pour obtenir des exemples de code utilisables pour charger un objet, consultez les rubriques suivantes. Pour utiliser ces exemples, vous devez mettre à jour les exemples de code et fournir des informations de chiffrement comme illustré dans le fragment de code précédent.

- Pour charger un objet en une seule opération, consultez Chargement d'objets dans un compartiment de répertoires.

- Pour les opérations d'API de chargement partitionné, consultez Utilisation du chargement partitionné avec les compartiments de répertoires.

Surveillance du chiffrement par défaut pour les compartiments de répertoires avec l' AWS CloudTrail

Vous pouvez suivre les demandes de configuration de chiffrement par défaut pour les compartiments Amazon S3 à l'aide d'événements AWS CloudTrail . Les noms d'événements d'API suivants sont utilisés dans CloudTrail les journaux :

- `PutBucketEncryption`
- `GetBucketEncryption`
- `DeleteBucketEncryption`

> **Note**
>
> - EventBridge n'est pas pris en charge dans les compartiments de répertoire.
> - Le chiffrement double couche côté serveur avec des clés AWS Key Management Service (AWS KMS) (DSSE-KMS) ou le chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C) ne sont pas pris en charge dans les compartiments d'annuaire.

Pour plus d'informations sur la surveillance du chiffrement par défaut avec AWS CloudTrail, consultez Surveillance du chiffrement par défaut avec Amazon AWS CloudTrail et Amazon EventBridge.

Utilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de répertoire

Les contrôles de sécurité intégrés AWS KMS peuvent vous aider à respecter les exigences de conformité liées au chiffrement. Vous pouvez choisir de configurer les compartiments de répertoire pour utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) et d'utiliser ces clés KMS pour protéger vos données dans les compartiments d'annuaire Amazon S3. Pour en savoir plus sur SSE-KMS, consultez Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

Autorisations

Pour charger ou télécharger un objet chiffré AWS KMS key à destination ou en provenance d'Amazon S3, vous avez besoin `kms:GenerateDataKey` d'`kms:Decrypt`autorisations sur la clé. Pour plus d'informations, consultez Permettre aux utilisateurs de clés d'utiliser une clé KMS pour les opérations de chiffrement dans le Guide de l'utilisateur AWS Key Management Service . Pour plus d'informations sur les AWS KMS autorisations requises pour les téléchargements partitionnés, consultez. API de chargement partitionné et autorisations

Pour plus d'informations sur les clés KMS pour SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS).

Rubriques

- AWS KMS keys
- Utilisation de SSE-KMS pour les opérations intercomptes
- Clés de compartiment Amazon S3
- Chiffrement SSE-KMS requis
- Contexte de chiffrement
- Envoi de demandes pour des objets AWS KMS chiffrés
- Audit du chiffrement SSE-KMS dans les compartiments de répertoires
- Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) pour les chargements de nouveaux objets dans des compartiments de répertoires

AWS KMS keys

Votre configuration SSE-KMS ne peut prendre en charge qu'une seule clé gérée par le client par compartiment de répertoires pendant toute la durée de vie du compartiment. La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. De même, après avoir spécifié une clé gérée par le client pour SSE-KMS, vous ne pouvez pas remplacer la clé gérée par le client pour la configuration SSE-KMS du compartiment.

Vous pouvez identifier la clé gérée par le client que vous avez spécifiée pour la configuration SSE-KMS du compartiment de la manière suivante :

- Effectuez une demande d'opération d'API `HeadObject` pour trouver la valeur de `x-amz-server-side-encryption-aws-kms-key-id` dans la réponse.

Pour utiliser une nouvelle clé gérée par le client pour vos données, nous vous recommandons de copier vos objets existants dans un nouveau compartiment de répertoires avec une nouvelle clé gérée par le client.

Lorsque vous spécifiez une cléAWS KMS gérée par le client pour le chiffrement dans votre compartiment de répertoires, utilisez uniquement l'ID ou l'ARN de la clé. Le format de l'alias de la clé KMS n'est pas pris en charge.

Pour plus d'informations sur les clés KMS pour SSE-KMS, consultez AWS KMS keys.

Utilisation de SSE-KMS pour les opérations intercomptes

Lors de l'utilisation du chiffrement pour les opérations intercomptes, tenez compte des éléments suivants :

- Si vous souhaitez accorder un accès intercompte à vos objets S3, configurez une politique de clé gérée par le client pour autoriser l'accès à partir d'un autre compte.
- Pour spécifier une clé gérée par le client, vous devez utiliser un ARN de clé KMS complet.

Clés de compartiment Amazon S3

Les clés de compartiment S3 sont toujours activées pour les opérations `GET` et `PUT` dans un compartiment de répertoires et ne peuvent pas être désactivées. Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de CopyObject, d'UploadPartCopy, de l'opération Copy dans les opérations par lot ou des tâches import. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS.

Pour les opérations d'API du point de terminaison zonal (au niveau de l'objet), à l'exception de CopyObjectet UploadPartCopy, vous authentifiez et autorisez les demandes pour une faible latence. CreateSession Nous recommandons que le chiffrement par défaut du compartiment utilise la configuration de chiffrement souhaitée et que vous ne remplaciez pas le chiffrement par défaut du compartiment dans vos demandes `CreateSession` ni dans vos demandes d'objets `PUT`. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. Pour chiffrer de nouveaux objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). Ensuite, lorsqu'une session

sera créée pour les opérations de l'API de point de terminaison zonal, les nouveaux objets seront automatiquement chiffrés et déchiffrés avec les clés SSE-KMS et les clés de compartiment S3 pendant la session. Pour plus d'informations sur les comportements de remplacement du chiffrement dans les compartiments de répertoire, voir Spécifier le chiffrement côté serveur avec AWS KMS pour les téléchargements de nouveaux objets.

Les clés de compartiment S3 sont utilisées pendant une période limitée dans le temps dans Amazon S3, ce qui réduit encore la nécessité pour Amazon S3 de faire des demandes AWS KMS pour effectuer des opérations de chiffrement. Pour plus d'informations sur l'utilisation des clés de compartiment S3, consultez Clés de compartiment Amazon S3 et Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

Chiffrement SSE-KMS requis

Pour exiger le chiffrement SSE-C de tous les objets figurant dans un compartiment de répertoires particulier, vous pouvez utiliser une politique de compartiment. Par exemple, lorsque vous utilisez l'opération d'API `CreateSession` pour autoriser le chargement d'un nouvel objet (`PutObject`, `CopyObject` et `CreateMultipartUpload`), la politique de compartiment suivante refuse l'autorisation de chargement de l'objet (`s3express:CreateSession`) à tout le monde si la demande `CreateSession` ne contient pas d'en-tête `x-amz-server-side-encryption-aws-kms-key-id` demandant le chiffrement SSE-KMS.

JSON

```
{
   "Version":"2012-10-17",
   "Id":"UploadObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3express:CreateSession",
         "Resource":"arn:aws:s3express:aws-region:111122223333:bucket/amzn-s3-
demo-bucket--usw2-az1--x-s3/*",
         "Condition":{
            "Null":{
               "s3express:x-amz-server-side-encryption-aws-kms-key-id":"true"
            }
         }
      }
```

```
    ]
}
```

Pour exiger qu'une donnée AWS KMS key soit utilisée pour chiffrer les objets d'un compartiment, vous pouvez utiliser la clé de `s3express:x-amz-server-side-encryption-aws-kms-key-id` condition. Pour spécifier la clé KMS, vous devez utiliser une clé Amazon Resource Name (ARN) au `arn:aws:kms:`*`region`*`:`*`acct-id`*`:key/`*`key-id` format suivant. AWS Identity and Access Management ne valide pas si la chaîne pour `s3express:x-amz-server-side-encryption-aws-kms-key-id` existe. L'ID de AWS KMS clé utilisé par Amazon S3 pour le chiffrement des objets doit correspondre à l'ID de AWS KMS clé indiqué dans la politique, sinon Amazon S3 refuse la demande.

Pour plus d'informations sur l'utilisation de SSE-KMS pour les chargements de nouveaux objets, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) pour les chargements de nouveaux objets dans des compartiments de répertoires.

Pour obtenir la liste complète des clés de condition spécifiques aux compartiments de répertoires, consultez Autorisation des opérations d'API de point de terminaison régional avec IAM.

Contexte de chiffrement

Pour les compartiments de répertoires, un contexte de chiffrement est un ensemble de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données. Aucune valeur supplémentaire de contexte de chiffrement n'est prise en charge. Pour plus d'informations sur le contexte de chiffrement, consultez la rubrique Contexte de chiffrement.

Par défaut, si vous utilisez SSE-KMS sur un compartiment de répertoires, Amazon S3 utilise l'Amazon Resource Name (ARN) de ce compartiment comme paire de contexte de chiffrement :

```
arn:aws:s3express:region:account-id:bucket/bucket-base-name--zone-id--x-s3
```

Assurez-vous que vos politiques IAM ou AWS KMS clés utilisent l'ARN de votre bucket comme contexte de chiffrement.

Vous pouvez éventuellement fournir une paire de contextes de chiffrement explicite en utilisant l'`x-amz-server-side-encryption-context`en-tête d'une demande d'API de point de terminaison zonal, telle que CreateSession. La valeur de cet en-tête est une chaîne codée en base64 d'un

fichier JSON codé en UTF-8, qui contient le contexte de chiffrement sous forme de paires clé-valeur. Pour les compartiments de répertoires, le contexte de chiffrement doit correspondre au contexte de chiffrement par défaut, à savoir l'Amazon Resource Name (ARN) du compartiment. De plus, étant donné que le contexte de chiffrement n'est pas chiffré, assurez-vous qu'il ne contienne pas d'informations sensibles.

Vous pouvez utiliser le contexte de chiffrement pour identifier et classer vos opérations cryptographiques par catégorie. Vous pouvez également utiliser la valeur ARN du contexte de chiffrement par défaut pour suivre les demandes pertinentes en AWS CloudTrail visualisant quel ARN de compartiment de répertoire a été utilisé avec quelle clé de chiffrement.

Dans le `requestParameters` champ d'un fichier CloudTrail journal, si vous utilisez SSE-KMS sur un bucket de répertoire, la valeur du contexte de chiffrement est l'ARN du bucket.

```
"encryptionContext": {
    "aws:s3express:arn": "arn:aws:s3:::arn:aws:s3express:region:account-
id:bucket/bucket-base-name--zone-id--x-s3"
}
```

En outre, pour le chiffrement d'objets avec SSE-KMS dans un bucket de répertoire, vos AWS KMS CloudTrail événements enregistrent l'ARN de votre bucket au lieu de celui de votre objet.

Envoi de demandes pour des objets AWS KMS chiffrés

Les compartiments de répertoires sont accessibles uniquement via HTTPS (TLS). En outre, les compartiments d'annuaire signent les demandes à l'aide de AWS Signature Version 4 (SigV4). Pour plus d'informations sur l'envoi de demandes d'objets AWS KMS chiffrés, consultezEnvoi de demandes pour des objets AWS KMS chiffrés.

Si votre objet utilise SSE-KMS, n'envoyez pas d'en-têtes de chiffrement pour les requêtes `GET` et `HEAD`. Sinon, vous obtiendrez une erreur HTTP 400 Bad Request (HTTP 400 Requête erronée).

Audit du chiffrement SSE-KMS dans les compartiments de répertoires

Pour vérifier l'utilisation de vos AWS KMS clés pour vos données cryptées SSE-KMS, vous pouvez utiliser AWS CloudTrail des journaux. Vous pouvez obtenir un aperçu de vos opérations cryptographiques, telles que GenerateDataKeyet Decrypt. CloudTrail prend en charge de nombreuses valeurs d'attribut pour filtrer votre recherche, notamment le nom de l'événement, le nom d'utilisateur et la source de l'événement.

Rubriques

- Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) pour les chargements de nouveaux objets dans des compartiments de répertoires

Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS) pour les chargements de nouveaux objets dans des compartiments de répertoires

Pour les compartiments d'annuaire, pour chiffrer vos données à l'aide du chiffrement côté serveur, vous pouvez utiliser soit le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3) (par défaut), soit le chiffrement côté serveur avec des clés () (SSE-KMS). AWS Key Management Service AWS KMS Nous recommandons que le chiffrement par défaut du compartiment utilise la configuration de chiffrement souhaitée et que vous ne remplaciez pas le chiffrement par défaut du compartiment dans vos demandes `CreateSession` ni dans vos demandes d'objets PUT. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. Pour plus d'informations sur les comportements de remplacement du chiffrement dans les compartiments de répertoire, voir Spécifier le chiffrement côté serveur avec AWS KMS pour les téléchargements de nouveaux objets.

Le chiffrement est configuré par défaut pour tous les compartiments Amazon S3, et tous les nouveaux objets qui sont chargés dans un compartiment S3 sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment dans Amazon S3. Si vous souhaitez spécifier un type de chiffrement différent pour un compartiment de répertoires, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Pour chiffrer de nouveaux objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. Votre configuration SSE-KMS ne peut prendre en charge qu'une seule clé gérée par le client par compartiment de répertoires pendant toute la durée de vie du compartiment. Après avoir spécifié une clé gérée par le client pour SSE-KMS, vous ne pouvez pas remplacer cette clé pour la configuration SSE-KMS du compartiment. Ensuite, lorsque vous spécifierez les paramètres de chiffrement côté serveur pour les nouveaux objets avec SSE-KMS, vous devrez vous assurer que la clé de chiffrement est la clé gérée par le client que vous avez spécifiée pour la configuration de chiffrement par défaut du compartiment de répertoires. Pour utiliser une nouvelle clé gérée par le client pour vos données, nous vous recommandons de copier vos objets existants dans un nouveau compartiment de répertoires avec une nouvelle clé gérée par le client.

Vous pouvez appliquer le chiffrement lorsque vous chargez un nouvel objet ou copiez un objet existant. Si vous modifiez le chiffrement d'un objet, un nouvel objet est créé pour remplacer l'ancien.

Vous pouvez spécifier SSE-KMS à l'aide des opérations de l'API REST AWS SDKs, et du AWS Command Line Interface ()AWS CLI.

> **Note**
>
> - Pour les compartiments de répertoires, les comportements de remplacement du chiffrement sont les suivants :
>   - Lorsque vous utilisez CreateSessionl'API REST pour authentifier et autoriser les demandes d'API de point de terminaison zonal, à l'exception de CopyObjectet UploadPartCopy, vous pouvez remplacer les paramètres de chiffrement par SSE-S3 ou par SSE-KMS uniquement si vous avez précédemment spécifié le chiffrement par défaut du compartiment avec SSE-KMS.
>   - Lorsque vous utilisez CreateSessionwith the AWS CLI ou the AWS SDKs pour authentifier et autoriser des requêtes d'API de point de terminaison zonal, à l'exception de CopyObjectet UploadPartCopy, vous ne pouvez pas du tout annuler les paramètres de chiffrement.
>   - Lorsque vous faites des CopyObjectdemandes, vous pouvez remplacer les paramètres de chiffrement par SSE-S3 ou SSE-KMS uniquement si vous avez précédemment spécifié le chiffrement par défaut du compartiment avec SSE-KMS. Lorsque vous faites des UploadPartCopydemandes, vous ne pouvez pas annuler les paramètres de chiffrement.
> - Vous pouvez utiliser plusieurs régions AWS KMS keys dans Amazon S3. Cependant, Amazon S3 traite actuellement les clés multi-régions comme s'il s'agissait de clés à région unique et n'utilise pas les fonctions multi-régions de la clé. Pour plus d'informations, consultez Utilisation des clés multi-régions dans le Guide du développeur AWS Key Management Service .
> - Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez avoir l'autorisation d'utiliser cette clé. Pour plus d'informations sur les autorisations intercomptes pour les clés KMS, consultez Création de clés KMS que d'autres comptes peuvent utiliser dans le Guide du développeur AWS Key Management Service .

Utilisation de l'API REST

> **Note**
>
> Une seule clé gérée par le client est prise en charge par compartiment de répertoires pendant toute la durée de vie de ce compartiment. La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. Une fois que vous avez spécifié SSE-KMS comme configuration de chiffrement par défaut de votre compartiment avec une clé gérée par le client, vous ne pourrez plus modifier cette clé pour la configuration SSE-KMS du compartiment.

Pour les opérations d'API du point de terminaison zonal (au niveau de l'objet), à l'exception de CopyObjectet UploadPartCopy, vous authentifiez et autorisez les demandes pour une faible latence. CreateSession Nous recommandons que le chiffrement par défaut du compartiment utilise les configurations de chiffrement souhaitées et que vous ne remplaciez pas le chiffrement par défaut du compartiment dans vos demandes `CreateSession` ni dans vos demandes d'objets PUT. Les nouveaux objets seront ensuite automatiquement chiffrés avec les paramètres de chiffrement souhaités. Pour chiffrer de nouveaux objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). Ensuite, lorsqu'une session sera créée pour les opérations de l'API de point de terminaison zonal, les nouveaux objets seront automatiquement chiffrés et déchiffrés avec les clés SSE-KMS et les clés de compartiment S3 pendant la session. Pour plus d'informations sur les comportements de remplacement du chiffrement dans les compartiments de répertoire, voir Spécifier le chiffrement côté serveur avec AWS KMS pour les téléchargements de nouveaux objets.

Dans les appels d'API de point de terminaison zonaux (sauf CopyObjectet UploadPartCopy) utilisant l'API REST, vous ne pouvez pas remplacer les valeurs des paramètres de chiffrement (`x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id`x-amz-server-side-encryption-context, et`x-amz-server-side-encryption-bucket-key-enabled`) de la `CreateSession` demande. Il n'est pas nécessaire de spécifier explicitement les valeurs de ces paramètres de chiffrement dans les appels d'API de point de terminaison zonal. Amazon S3 utilisera les valeurs des paramètres de chiffrement de la demande `CreateSession` pour protéger les nouveaux objets dans le compartiment de répertoires.

> **Note**
>
> Lorsque vous utilisez le AWS CLI ou le AWS SDKs, pour`CreateSession`, le jeton de session est automatiquement actualisé pour éviter les interruptions de service à l'expiration d'une session. AWS CLI Ou AWS SDKs utilisez la configuration de chiffrement par défaut du compartiment pour la `CreateSession` demande. Il n'est pas possible de remplacer les valeurs des paramètres de chiffrement dans la demande `CreateSession`. De plus, dans les appels d'API du point de terminaison zonal (sauf CopyObjectet UploadPartCopy), il n'est pas possible de remplacer les valeurs des paramètres de chiffrement de la `CreateSession` demande.

En effet CopyObject, pour chiffrer de nouvelles copies d'objets dans un compartiment d'annuaire avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut du compartiment d'annuaire avec une clé KMS (en particulier, une clé gérée par le client). Ensuite, lorsque vous spécifierez les paramètres de chiffrement côté serveur pour les nouvelles copies d'objets avec SSE-KMS, vous devrez vous assurer que la clé de chiffrement est la clé gérée par le client que vous avez spécifiée pour la configuration de chiffrement par défaut du compartiment de répertoires. En effet UploadPartCopy, pour chiffrer de nouvelles copies partielles d'objets dans un compartiment d'annuaire avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut du compartiment d'annuaire avec une clé KMS (en particulier, une clé gérée par le client). Vous ne pouvez pas spécifier de paramètres de chiffrement côté serveur pour les nouvelles copies partielles d'objets avec SSE-KMS dans les en-têtes de demande. UploadPartCopy En outre, les paramètres de chiffrement que vous fournissez dans la CreateMultipartUploaddemande doivent correspondre à la configuration de chiffrement par défaut du compartiment de destination.

Rubriques

- Opérations d'API REST Amazon S3 prenant en charge SSE-KMS
- Contexte de chiffrement (x-amz-server-side-encryption-context)
- AWS KMS ID de clé (x-amz-server-side-encryption-aws-kms-key-id)
- Clés de compartiment S3 (x-amz-server-side-encryption-aws-bucket-key-enabled)

Opérations d'API REST Amazon S3 prenant en charge SSE-KMS

Les opérations d'API REST suivantes au niveau de l'objet dans les compartiments de répertoires acceptent les en-têtes de demande `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id` et `x-amz-server-side-encryption-context`.

- CreateSession— Lorsque vous utilisez les opérations d'API du point de terminaison zonal (au niveau de l'objet) (sauf CopyObject et UploadPartCopy), vous pouvez spécifier ces en-têtes de requête.
- PutObject – Lorsque vous chargez des données avec l'opération d'API PUT, vous pouvez spécifier ces en-têtes de demande.
- CopyObject – Lorsque vous copiez un objet, vous disposez d'un objet source et d'un objet cible. Lorsque vous transmettez les en-têtes SSE-KMS avec l'opération `CopyObject`, ils sont appliqués uniquement à l'objet cible.
- CreateMultipartUpload : lorsque vous chargez des objets volumineux avec l'opération d'API de chargement partitionné, vous pouvez spécifier ces en-têtes. Vous spécifiez ces en-têtes dans la demande `CreateMultipartUpload`.

Les en-têtes de réponse des opérations d'API REST suivantes renvoient l'en-tête `x-amz-server-side-encryption` lorsqu'un objet est stocké grâce au chiffrement côté serveur.

- CreateSession
- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - Toutes les demandes `GET` et `PUT` pour un objet protégé par AWS KMS échouent si vous ne les faites pas en utilisant le protocole TLS (Transport Layer Security) ou Signature Version 4.
> - Si votre objet utilise le SSE-KMS, n'envoyez pas d'en-têtes de demande de chiffrement pour les `GET` requêtes et les `HEAD` requêtes, sinon vous obtiendrez une erreur HTTP 400. BadRequest

Contexte de chiffrement (**`x-amz-server-side-encryption-context`**)

Si vous spécifiez `x-amz-server-side-encryption:aws:kms`, l'API Amazon S3 vous permet de fournir un contexte de chiffrement explicite avec l'en-tête `x-amz-server-side-encryption-context`. Pour les compartiments de répertoires, un contexte de chiffrement est un ensemble de paires clé-valeur qui contient des informations contextuelles supplémentaires sur les données. La valeur doit correspondre au contexte de chiffrement par défaut, à savoir l'Amazon Resource Name (ARN) du compartiment. Aucune valeur supplémentaire de contexte de chiffrement n'est prise en charge.

Pour plus d'informations sur le contexte de chiffrement dans les compartiments de répertoires, consultez Contexte de chiffrement. Pour des informations générales sur le contexte de chiffrement, consultez Concepts AWS Key Management Service - Contexte de chiffrement dans le Guide du développeur AWS Key Management Service .

AWS KMS ID de clé (**`x-amz-server-side-encryption-aws-kms-key-id`**)

Vous pouvez utiliser l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` pour spécifier l'ID de la clé gérée par le client utilisée pour protéger les données.

Votre configuration SSE-KMS ne peut prendre en charge qu'une seule clé gérée par le client par compartiment de répertoires pendant toute la durée de vie du compartiment. La Clé gérée par AWS (`aws/s3`) n'est pas prise en charge. De même, après avoir spécifié une clé gérée par le client pour SSE-KMS, vous ne pouvez pas remplacer la clé gérée par le client pour la configuration SSE-KMS du compartiment.

Vous pouvez identifier la clé gérée par le client que vous avez spécifiée pour la configuration SSE-KMS du compartiment de la manière suivante :

- Effectuez une demande d'opération d'API `HeadObject` pour trouver la valeur de `x-amz-server-side-encryption-aws-kms-key-id` dans la réponse.

Pour utiliser une nouvelle clé gérée par le client pour vos données, nous vous recommandons de copier vos objets existants dans un nouveau compartiment de répertoires avec une nouvelle clé gérée par le client.

Pour plus d'informations sur le contexte de chiffrement dans les compartiments de répertoires, consultez AWS KMS keys.

Clés de compartiment S3 (**`x-amz-server-side-encryption-aws-bucket-key-enabled`**)

Les clés de compartiment S3 sont toujours activées pour les opérations `GET` et `PUT` dans un compartiment de répertoires et ne peuvent pas être désactivées. Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de CopyObject, d'UploadPartCopy, de l'opération Copy dans les opérations par lot ou des tâches import. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS. Pour plus d'informations sur les clés de compartiment S3 dans les compartiments de répertoire, consultez Contexte de chiffrement.

À l'aide du AWS CLI

> **Note**
>
> Lorsque vous utilisez le symbole AWS CLI, for`CreateSession`, le jeton de session est automatiquement actualisé pour éviter les interruptions de service lors de l'expiration d'une session. Il n'est pas possible de remplacer les valeurs des paramètres de chiffrement pour la demande `CreateSession`. De plus, dans les appels d'API du point de terminaison zonal (sauf CopyObjectet UploadPartCopy), il n'est pas possible de remplacer les valeurs des paramètres de chiffrement de la `CreateSession` demande.
> Pour chiffrer de nouveaux objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). Ensuite, lorsqu'une session sera créée pour les opérations de l'API de point de terminaison zonal, les nouveaux objets seront automatiquement chiffrés et déchiffrés avec les clés SSE-KMS et les clés de compartiment S3 pendant la session.

Pour utiliser les exemples de AWS CLI commandes suivants, remplacez-les *user input placeholders* par vos propres informations.

Lorsque vous chargez un nouvel objet ou que vous copiez un objet existant, vous pouvez spécifier l'utilisation du chiffrement côté serveur avec des AWS KMS clés pour chiffrer vos données. Pour ce faire, utilisez la commande `put-bucket-encryption` afin de définir la configuration de chiffrement par défaut du compartiment de répertoires en tant que chiffrement SSE-KMS (`aws:kms`). Plus précisément, ajoutez l'en-tête `--server-side-encryption aws:kms` à la demande. Utilisez le `--ssekms-key-id` *example-key-id* pour ajouter la AWS KMS clé gérée par le client que vous avez créée. Si vous le spécifiez`--server-side-encryption aws:kms`, vous devez fournir un identifiant de AWS KMS clé pour votre clé gérée par le client. Les compartiments de répertoire n'utilisent pas de clé AWS gérée. Pour obtenir un exemple de commande, consultez À l'aide du AWS CLI.

Ensuite, lorsque vous chargez un nouvel objet à l'aide de la commande suivante, Amazon S3 utilise les paramètres du compartiment pour le chiffrement par défaut afin de chiffrer l'objet par défaut.

```
aws s3api put-object --bucket bucket-base-name--zone-id--x-s3 --key example-object-key
 --body filepath
```

Vous n'avez pas besoin d'ajouter `-\-bucket-key-enabled` explicitement dans les commandes d'opérations d'API de point de terminaison zonal. Les clés de compartiment S3 sont toujours activées pour les opérations `GET` et `PUT` dans un compartiment de répertoires et ne peuvent pas être désactivées. Les clés de compartiment S3 ne sont pas prises en charge lorsque vous copiez des objets chiffrés avec SSE-KMS depuis des compartiments à usage général vers des compartiments de répertoires, depuis des compartiments de répertoires vers des compartiments à usage général ou entre des compartiments de répertoires, par le biais de CopyObject, d'UploadPartCopy, de l'opération Copy dans les opérations par lot ou des tâches import. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande de copie est faite pour un objet chiffré par KMS.

Vous pouvez copier un objet d'un compartiment source (par exemple, un compartiment à usage général) vers un nouveau compartiment (par exemple, un compartiment de répertoires) et utiliser le chiffrement SSE-KMS pour les objets de destination. Pour ce faire, utilisez la commande `put-bucket-encryption` afin de définir la configuration de chiffrement par défaut du compartiment de destination en tant que chiffrement SSE-KMS (`aws:kms`). Pour obtenir un exemple de commande, consultez À l'aide du AWS CLI. Ensuite, lorsque vous copiez un objet à l'aide de la commande suivante, Amazon S3 utilise les paramètres du compartiment pour le chiffrement par défaut afin de chiffrer l'objet par défaut.

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket/example-object-key --
bucket bucket-base-name--zone-id--x-s3 --key example-object-key
```

En utilisant le AWS SDKs

Lors de l'utilisation AWS SDKs, vous pouvez demander à Amazon S3 de l'utiliser AWS KMS keys pour le chiffrement côté serveur. Les exemples suivants montrent comment utiliser SSE-KMS avec AWS SDKs pour Java et .NET. Pour plus d'informations sur les autres SDKs, consultez la section Exemples de code et de bibliothèques sur le AWS Developer Center.

> **Note**
>
> Lorsque vous utilisez le symbole AWS SDKs, for`CreateSession`, le jeton de session est automatiquement actualisé pour éviter les interruptions de service lors de l'expiration d'une session. Il n'est pas possible de remplacer les valeurs des paramètres de chiffrement pour la demande `CreateSession`. De plus, dans les appels d'API du point de terminaison zonal (sauf CopyObjectet UploadPartCopy), il n'est pas possible de remplacer les valeurs des paramètres de chiffrement de la `CreateSession` demande.
> Pour chiffrer de nouveaux objets dans un compartiment de répertoires avec SSE-KMS, vous devez spécifier SSE-KMS comme configuration de chiffrement par défaut de ce compartiment avec une clé KMS (plus spécifiquement, une clé gérée par le client). Ensuite, lorsqu'une session sera créée pour les opérations de l'API de point de terminaison zonal, les nouveaux objets seront automatiquement chiffrés et déchiffrés avec les clés SSE-KMS et les clés de compartiment S3 pendant la session.
> Pour plus d'informations sur l'utilisation AWS SDKs de la configuration de chiffrement par défaut d'un bucket d'annuaire en tant que SSE-KMS, consultez. En utilisant le AWS SDKs

> **Important**
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 ne prend en charge que les clés KMS à chiffrement symétrique. Pour plus d'informations sur ces clés, consultez Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur la création de clés gérées par le client, consultez la section Programmation de l' AWS KMS API dans le Guide du AWS Key Management Service développeur.

Chiffrement en transit

Les compartiments de répertoires utilisent des points de terminaison d'API régionaux et zonaux. Selon l'opération d'API Amazon S3 que vous utilisez, un point de terminaison régional ou zonal est requis. Vous pouvez accéder aux points de terminaison zonaux et régionaux via un point de terminaison de cloud privé virtuel (VPC) de passerelle. Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle. Pour en savoir plus sur les points de terminaison d'API régionaux et zonaux, consultez Mise en réseau des compartiments de répertoires.

Suppression de données

Vous pouvez supprimer un ou plusieurs objets directement depuis vos compartiments de répertoire à l'aide de la console Amazon S3 AWS SDKs, AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. Étant donné que tous les objets figurant dans les compartiments de répertoires entraînent des coûts de stockage, nous vous recommandons de supprimer les objets dont vous n'avez plus besoin.

La suppression d'un objet stocké dans un compartiment de répertoires supprime également de manière récursive tous les répertoires parents, si ces répertoires parents ne contiennent aucun objet autre que l'objet en cours de suppression.

> **Note**
>
> La suppression par authentification multifactorielle (MFA) et la gestion des versions S3 ne sont pas prises en charge pour S3 Express One Zone.

Authentification et autorisation des demandes

Par défaut, les compartiments de répertoires sont privés et sont accessibles uniquement par les utilisateurs auxquels l'accès a été explicitement accordé. La limite de contrôle d'accès pour les compartiments de répertoires est définie uniquement au niveau compartiment. En revanche, la limite de contrôle d'accès pour les compartiments à usage général peut être définie au niveau des compartiments, du préfixe ou de la balise d'objet. Cette différence signifie que les compartiments de répertoires sont la seule ressource que vous pouvez inclure dans les politiques de compartiment ou les politiques d'identité IAM pour accéder à S3 Express One Zone.

Amazon S3 Express One Zone prend en charge à la fois l'autorisation AWS Identity and Access Management (AWS IAM) et l'autorisation basée sur les sessions :

- Pour utiliser les opérations d'API de point de terminaison régional (opérations au niveau des compartiments ou du plan de contrôle) avec S3 Express One Zone, vous utilisez le modèle d'autorisation IAM, qui n'implique aucune gestion des sessions. Les autorisations sont accordées pour les actions, de façon individuelle. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM.
- Pour utiliser les opérations d'API de point de terminaison zonal (opérations de niveau objet ou plan de données), à l'exception de `CopyObject` et de `HeadBucket`, utilisez l'opération d'API `CreateSession` pour créer et gérer des sessions optimisées afin d'autoriser les demandes de données à faible latence. Pour récupérer et utiliser un jeton de session, vous devez autoriser l'action `s3express:CreateSession` pour votre compartiment de répertoires dans une politique basée sur l'identité ou une politique de compartiment. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM. Si vous accédez à S3 Express One Zone dans la console Amazon S3, via le AWS Command Line Interface (AWS CLI), ou en utilisant le AWS SDKs, S3 Express One Zone crée une session en votre nom.

L'opération d'API `CreateSession`vous permet d'authentifier et d'autoriser les demandes par le biais d'un nouveau mécanisme basé sur les sessions. Vous pouvez utiliser `CreateSession` pour demander des informations d'identification temporaires afin de bénéficier d'un accès à faible latence à votre compartiment. Ces informations d'identification temporaires sont limitées à un compartiment de répertoires spécifique.

Pour travailler avec`CreateSession`, nous vous recommandons d'utiliser la dernière version du AWS SDKs ou d'utiliser le AWS Command Line Interface (AWS CLI). L'établissement, le rafraîchissement AWS SDKs et la AWS CLI résiliation des sessions pris en charge et gérés en votre nom.

Vous utilisez des jetons de session avec uniquement des opérations zonales (niveau objet) (à l'exception de `CopyObject` et `HeadBucket`) pour répartir la latence associée à l'autorisation sur un certain nombre de demandes dans une session. Pour les opérations d'API de point de terminaison régional (opérations de niveau compartiment), vous utilisez l'autorisation IAM, qui n'implique pas la gestion d'une session. Pour plus d'informations, consultez Autorisation des opérations d'API de point de terminaison régional avec IAM et Autorisation des opérations d'API de point de terminaison zonal avec `CreateSession`.

Comment les opérations d'API sont autorisées et authentifiées

Le tableau suivant répertorie les informations d'autorisation et d'authentification pour les opérations d'API des compartiments de répertoires. Pour chaque opération d'API, le tableau indique le nom de l'opération d'API, l'action de politique IAM, le type de point de terminaison (régional ou zonal) et le mécanisme d'autorisation (IAM ou basé sur une session). Ce tableau indique également les endroits où l'accès intercompte est pris en charge. L'accès aux actions de niveau compartiment peut être accordé uniquement dans des politiques basées sur l'identité IAM (utilisateur ou rôle), et non pas dans des politiques de compartiment.

« Hello, World! »	Type de point de terminaison	Action IAM	Accès intercomptes
`CreateBucket`	Régional	`s3express:CreateBucket`	Non
`DeleteBucket`	Régional	`s3express:DeleteBucket`	Non
`ListDirectoryBuckets`	Régional	`s3express:ListAllMyDirectoryBuckets`	Non
`PutBucketPolicy`	Régional	`s3express:PutBucketPolicy`	Non
`GetBucketPolicy`	Régional	`s3express:GetBucketPolicy`	Non
`DeleteBucketPolicy`	Régional	`s3express:DeleteBucketPolicy`	Non
`CreateSession`	Zonal	`s3express:CreateSession`	Oui
`CopyObject`	Zonal	`s3express:CreateSession`	Oui
`DeleteObject`	Zonal	`s3express:CreateSession`	Oui
`DeleteObjects`	Zonal	`s3express:CreateSession`	Oui
`HeadObject`	Zonal	`s3express:CreateSession`	Oui

« Hello, World! »	Type de point de terminaison	Action IAM	Accès intercomptes
PutObject	Zonal	s3express:CreateSession	Oui
RenameObject	Zonal	s3express:CreateSession	Non
GetObjectAttributes	Zonal	s3express:CreateSession	Oui
ListObjectsV2	Zonal	s3express:CreateSession	Oui
HeadBucket	Zonal	s3express:CreateSession	Oui
CreateMultipartUpload	Zonal	s3express:CreateSession	Oui
UploadPart	Zonal	s3express:CreateSession	Oui
UploadPartCopy	Zonal	s3express:CreateSession	Oui
CompleteMultipartUpload	Zonal	s3express:CreateSession	Oui
AbortMultipartUpload	Zonal	s3express:CreateSession	Oui
ListParts	Zonal	s3express:CreateSession	Oui
ListMultipartUploads	Zonal	s3express:CreateSession	Oui
ListAccessPointsForDirectoryBuckets	Zonal	s3express:ListAccessPointsForDirectoryBuckets	Oui

« Hello, World! »	Type de point de terminaison	Action IAM	Accès intercomptes
`GetAccessPointScope`	Zonal	`s3express:GetAccessPointScope`	Oui
`PutAccessPointScope`	Zonal	`s3express:PutAccessPointScope`	Oui
`DeleteAccessPointScope`	Zonal	`s3express:DeleteAccessPointScope`	Oui

Rubriques

- Autorisation des opérations d'API de point de terminaison régional avec IAM
- Autorisation des opérations d'API de point de terminaison zonal avec CreateSession

Autorisation des opérations d'API de point de terminaison régional avec IAM

AWS Identity and Access Management (IAM) est un outil Service AWS qui aide les administrateurs à contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources Amazon S3 dans les compartiments d'annuaire et les opérations S3 Express One Zone. Vous pouvez utiliser IAM sans frais supplémentaires.

Par défaut, les utilisateurs ne disposent pas d'autorisations pour les compartiments de répertoires. Pour accorder des autorisations d'accès pour les compartiments de répertoires, vous pouvez utiliser IAM pour créer des utilisateurs, des groupes ou des rôles, et attacher des autorisations à ces identités. Pour plus d'informations sur IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Pour fournir l'accès, vous pouvez ajouter des autorisations à vos utilisateurs, groupes ou rôles via les méthodes suivantes :

- Utilisateurs et groupes dans AWS IAM Identity Center : créez un ensemble d'autorisations. Suivez les instructions de la rubrique Création d'un jeu d'autorisations du Guide de l'utilisateur AWS IAM Identity Center .
- Utilisateurs gérés dans IAM via un fournisseur d'identité : créez un rôle pour la fédération d'identité. Pour plus d'informations, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM.
- Rôles et utilisateurs IAM : créez un rôle que votre utilisateur peut endosser. Suivez les instructions fournies dans Création d'un rôle pour la délégation d'autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur IAM pour S3 Express One Zone, consultez les rubriques suivantes.

Rubriques

- Principaux
- Ressources
- Actions spécifiques aux compartiments de répertoires
- Politiques IAM basées sur l'identité pour les compartiments de répertoires
- Exemples de politiques de compartiment pour les compartiments de répertoires

Principaux

Lorsque vous créez une politique basée sur les ressources pour accorder l'accès à vos compartiments, vous devez utiliser l'élément `Principal` pour spécifier la personne ou l'application qui peut effectuer une demande d'action ou d'opération sur cette ressource. Pour des politiques de compartiment de répertoires, vous pouvez utiliser les principaux suivants :

- Un AWS compte
- Un utilisateur IAM
- Un rôle IAM
- Un utilisateur fédéré

Pour plus d'informations, consultez Principal dans le Guide de l'utilisateur IAM.

Ressources

Amazon Resource Names (ARNs) pour les compartiments de répertoire contient l'`s3express`espace de noms Région AWS, l'ID de AWS compte et le nom du compartiment de répertoire, qui inclut l'ID de AWS zone. (une zone de disponibilité ou un identifiant de zone locale).

Pour accéder à votre compartiment de répertoires et y effectuer des actions, vous devez utiliser le format d'ARN suivant :

```
arn:aws:s3express:region:account-id:bucket/base-bucket-name--zone-id--x-s3
```

Pour accéder à votre point d'accès à un bucket de répertoire et y effectuer des actions, vous devez utiliser le format ARN suivant :

```
arn:aws::s3express:region:account-id:accesspoint/accesspoint-basename--zone-id--xa-s3
```

Pour plus d'informations ARNs, consultez le guide Amazon Resource Names (ARNs)de l'utilisateur IAM. Pour plus d'informations sur les ressources, consultez Éléments de politique JSON IAM : Resource dans le Guide de l'utilisateur IAM.

Actions spécifiques aux compartiments de répertoires

Dans une politique basée sur l'identité IAM ou sur les ressources, vous définissez quelles actions S3 sont autorisées ou refusées. Les actions correspondent à des opérations d'API spécifiques. Avec les compartiments de répertoire, vous devez utiliser l'espace de noms S3 Express One Zone pour accorder des autorisations, appelé. `s3express`

Lorsque vous autorisez l'`s3express:CreateSession`autorisation, l'opération d'`CreateSession`API récupère un jeton de session temporaire pour toutes les opérations de l'API de point de terminaison zonal (niveau objet). Le jeton de session renvoie les informations d'identification qui sont utilisées pour toutes les autres opérations de l'API Zonal Endpoint. Par conséquent, vous n'accordez pas d'autorisations d'accès aux opérations d'API zonales avec des politiques IAM. `CreateSession`Permet plutôt l'accès à toutes les opérations au niveau de l'objet. Pour obtenir la liste des opérations et des autorisations de l'API zonale, consultez Authentification et autorisation des demandes.

Pour en savoir plus sur l'opération d'API `CreateSession`, consultez CreateSession dans la Référence d'API Amazon Simple Storage Service.

Vous pouvez indiquer les actions suivantes dans l'élément `Action` d'une déclaration de politique IAM. Utilisez des politiques pour accorder des autorisations permettant d'effectuer une opération dans AWS. Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API du même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations d'API. L'accès aux actions de niveau compartiment peut être accordé uniquement dans des politiques basées sur l'identité IAM (utilisateur ou rôle) et non pas dans des politiques de compartiment.

Pour plus d'informations sur la configuration de stratégies de point d'accès, consultez Configuration des politiques IAM pour l'utilisation des points d'accès pour les compartiments d'annuaire.

Pour plus d'informations, consultez Actions, ressources et clés de condition pour Amazon S3 Express.

Politiques IAM basées sur l'identité pour les compartiments de répertoires

Avant de créer des compartiments de répertoires, vous devez accorder les autorisations nécessaires à votre rôle ou à vos utilisateurs AWS Identity and Access Management (IAM). Cet exemple de politique autorise l'accès à l'opération d'API `CreateSession` (à utiliser avec les opérations d'API de point de terminaison zonal [niveau objet]) et à toutes les opérations d'API de point de terminaison régional (niveau compartiment). Cette politique autorise l'utilisation de l'opération d'API `CreateSession` avec tous les compartiments de répertoires, mais les opérations d'API de point de terminaison régional sont autorisées à être utilisées uniquement avec le compartiment de répertoires spécifié. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAccessRegionalEndpointAPIs",
            "Effect": "Allow",
            "Action": [
                "s3express:DeleteBucket",
                "s3express:DeleteBucketPolicy",
                "s3express:CreateBucket",
                "s3express:PutBucketPolicy",
```

```
                "s3express:GetBucketPolicy",
                "s3express:ListAllMyDirectoryBuckets"
            ],

            "Resource": "arn:aws:s3express:region:account_id:bucket/example-s3-
directory-bucket;/*"
        },
        {
            "Sid": "AllowCreateSession",
            "Effect": "Allow",
            "Action": "s3express:CreateSession",
            "Resource": "*"
        }
    ]
 }
```

Exemples de politiques de compartiment pour les compartiments de répertoires

Cette section fournit des exemples de politiques pour les compartiments de répertoires. Pour utiliser ces politiques, remplacez les *user input placeholders* par vos propres informations.

L'exemple de politique de compartiment suivant permet *111122223333* à Compte AWS ID d'utiliser l'opération d'`CreateSession`API avec la `ReadWrite` session par défaut pour le compartiment de répertoire spécifié. Cette politique accorde l'accès aux opérations d'API de point de terminaison zonal (niveau objet).

Example – Politique de compartiment permettant d'autoriser les appels **`CreateSession`** avec la session **`ReadWrite`** par défaut

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadWriteAccess",
            "Effect": "Allow",
            "Resource": "arn:aws:s3express:us-west-2:account-id:bucket/amzn-s3-
demo-bucket--usw2-az1--x-s3",
            "Principal": {
```

```
                "AWS": [
                    "111122223333"
                ]
            },
            "Action": [
                "s3express:CreateSession"
            ]
        }
    ]
}
```

Example – Politique de compartiment permettant d'autoriser les appels **`CreateSession`** avec une session **`ReadOnly`**

L'exemple de politique de bucket suivant permet *111122223333* à Compte AWS ID d'utiliser l'opération `CreateSession` d'API. Cette politique utilise la clé de condition `s3express:SessionMode` avec la valeur `ReadOnly` pour définir une session en lecture seule.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ReadOnlyAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": "s3express:CreateSession",
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "s3express:SessionMode": "ReadOnly"
                }
            }
        }
    ]
}
```

Example – Politique de compartiment permettant d'autoriser l'accès intercompte pour les appels **`CreateSession`**

L'exemple de politique de compartiment suivant permet *111122223333* à Compte AWS ID d'utiliser l'opération d'`CreateSession`API pour le compartiment de répertoire spécifié qui appartient à Compte AWS ID*444455556666*.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccount",
            "Effect": "Allow",
            "Principal": {
                "AWS": "111122223333"
            },
            "Action": [
                "s3express:CreateSession"
            ],
            "Resource": "arn:aws:s3express:us-west-2:444455556666:bucket/amzn-s3-
demo-bucket--usw2-az1--x-s3"

        }
    ]
}
```

Autorisation des opérations d'API de point de terminaison zonal avec **`CreateSession`**

Pour utiliser les opérations d'API de point de terminaison zonal (opérations de niveau objet ou plan de données), à l'exception de `CopyObject` et de `HeadBucket`, utilisez l'opération d'API `CreateSession` pour créer et gérer des sessions optimisées afin d'autoriser les demandes de données à faible latence. Pour récupérer et utiliser un jeton de session, vous devez autoriser l'action

`s3express:CreateSession` pour votre compartiment de répertoires dans une politique basée sur l'identité ou une politique de compartiment. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM. Si vous accédez à S3 Express One Zone dans la console Amazon S3, via le AWS Command Line Interface (AWS CLI), ou en utilisant le AWS SDKs, S3 Express One Zone crée une session en votre nom. Toutefois, vous ne pouvez pas modifier le `SessionMode` paramètre lorsque vous utilisez le AWS CLI ou AWS SDKs.

Si vous utilisez l'API REST Amazon S3, vous pouvez ensuite utiliser l'opération d'API `CreateSession` pour obtenir des informations d'identification de sécurité temporaires qui incluent un ID de clé d'accès, une clé d'accès secrète, un jeton de session et une date d'expiration. Les informations d'identification temporaires fournissent les mêmes autorisations que les informations d'identification de sécurité à long terme, telles que les informations d'identification d'utilisateur IAM, mais les informations d'identification de sécurité temporaires doivent inclure un jeton de session.

Mode session

Le mode session définit l'étendue de la session. Dans votre politique de compartiment, vous pouvez spécifier la clé de condition `s3express:SessionMode` pour contrôler qui peut créer une session `ReadWrite` ou `ReadOnly`. Pour plus d'informations sur les sessions `ReadWrite` et `ReadOnly`, consultez le paramètre `x-amz-create-session-mode` pour CreateSession dans la Référence d'API Amazon S3. Pour plus d'informations sur la politique de compartiment à créer, consultez Exemples de politiques de compartiment pour les compartiments de répertoires.

Jeton de session

Lorsque vous effectuez un appel en utilisant des informations d'identification de sécurité temporaires, l'appel doit inclure un jeton de session. Le jeton de session est renvoyé avec les informations d'identification temporaires. Un jeton de session est limité à votre compartiment de répertoires et est utilisé pour vérifier que les informations d'identification de sécurité sont valides et n'ont pas expiré. Pour protéger vos sessions, les informations d'identification de sécurité temporaires expirent au bout de 5 minutes.

`CopyObject` et **`HeadBucket`**

Les informations d'identification de sécurité temporaires sont limitées à un compartiment de répertoires spécifique et sont automatiquement activées pour tous les appels d'API d'opérations zonales (niveau objet) vers un compartiment de répertoires donné. Contrairement aux autres opérations d'API de point de terminaison zonal, `CopyObject` et `HeadBucket` n'utilisent pas l'authentification `CreateSession`. Toutes les demandes `CopyObject` et `HeadBucket` doivent être authentifiées et signées au moyen d'informations d'identification IAM. Toutefois, `CopyObject`

et `HeadBucket` sont toujours autorisées par `s3express:CreateSession`, comme les autres opérations d'API de point de terminaison zonal.

Pour plus d'informations, consultez CreateSession dans la Référence d'API Amazon Simple Storage Service.

Bonnes pratiques de sécurité pour les compartiments de répertoires

Il existe différentes fonctionnalités de sécurité à prendre en compte lorsque vous travaillez avec des compartiments de répertoires. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des recommandations utiles plutôt que comme des prescriptions.

Paramètres de blocage d'accès public définis par défaut et de propriété des objets

Les compartiments de répertoires prennent en charge le blocage de l'accès public S3 et la propriété des objets S3. Ces fonctionnalités S3 sont utilisées pour auditer et gérer l'accès à vos compartiments et objets.

Par défaut, tous les paramètres de blocage de l'accès public des compartiments de répertoires sont activés. En outre, la propriété de l'objet est définie pour être appliquée par le propriétaire du compartiment, ce qui signifie que les listes de contrôle d'accès (ACLs) sont désactivées. Ces paramètres ne peuvent pas être modifiés. Pour plus d'informations sur ces fonctionnalités, consultez the section called "Blocage de l'accès public" et the section called "Contrôle de la propriété des objets".

> **Note**
>
> Vous ne pouvez pas autoriser l'accès aux objets stockés dans des compartiments de répertoires. Vous pouvez accorder l'accès uniquement à vos compartiments de répertoires. Le modèle d'autorisation pour S3 Express One Zone est différent du modèle d'autorisation pour Amazon S3. Pour plus d'informations, consultez Autorisation des opérations d'API de point de terminaison zonal avec `CreateSession`.

Authentification et autorisation

Les mécanismes d'authentification et d'autorisation pour les compartiments de répertoires diffèrent selon que vous envoyez des demandes aux opérations d'API de point de terminaison zonal ou aux

opérations d'API de point de terminaison régional. Les opérations d'API zonales sont des opérations de niveau objet (plan de données). Les opérations d'API régionales sont des opérations de niveau compartiment (plan de contrôle).

Vous authentifiez et autorisez les demandes adressées aux opérations d'API de point de terminaison zonal par le biais d'un nouveau mécanisme basé sur les sessions, optimisé pour fournir une latence minimale. Avec l'authentification basée sur les sessions, ils AWS SDKs utilisent l'opération `CreateSession` API pour demander des informations d'identification temporaires qui fournissent un accès à faible latence à votre compartiment d'annuaire. Ces informations d'identification temporaires sont limitées à un compartiment de répertoires spécifique et expirent au bout de 5 minutes. Vous pouvez utiliser ces informations d'identification temporaires pour signer des appels d'API zonaux (niveau objet). Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison zonal avec `CreateSession`.

Signature des demandes avec des informations d'identification pour la gestion des compartiments de répertoires

Vous utilisez vos informations d'identification pour signer les demandes d'API du point de terminaison zonal (niveau objet) avec AWS Signature Version 4, avec `s3express` comme nom de service. Lorsque vous signez vos demandes, utilisez la clé secrète renvoyée par `CreateSession` et fournissez également le jeton de session avec `x-amzn-s3session-token` `header`. Pour de plus amples informations, veuillez consulter CreateSession.

Les personnes prises en charge AWS SDKs gèrent les informations d'identification et la signature en votre nom. Nous vous recommandons d'utiliser le AWS SDKs pour actualiser les informations d'identification et signer les demandes pour vous.

Signature de demandes avec des informations d'identification IAM

Tous les appels d'API régionaux (niveau compartiment) doivent être authentifiés et signés par des informations d'identification AWS Identity and Access Management (IAM) plutôt que par des informations d'identification de session temporaires. Les informations d'identification IAM comprennent l'ID de clé d'accès et la clé d'accès secrète des identités IAM. Toutes les demandes `CopyObject` et `HeadBucket` doivent également être authentifiées et signées au moyen d'informations d'identification IAM.

Pour réduire au maximum la latence de vos appels d'opérations zonaux (niveau objet), nous vous recommandons d'utiliser les informations d'identification obtenues lors de l'appel de `CreateSession` pour signer vos demandes, à l'exception des demandes adressées à `CopyObject` et `HeadBucket`.

Utiliser AWS CloudTrail

AWS CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS dans Amazon S3. Vous pouvez utiliser les informations collectées par CloudTrail pour déterminer les éléments suivants :

- La demande qui a été adressée à Amazon S3
- L'adresse IP à partir de laquelle la demande a été effectuée
- La personne ayant effectué la demande
- La date et l'heure où la demande a été effectuée
- Des détails supplémentaires sur la demande

Lorsque vous configurez votre Compte AWS, les événements CloudTrail de gestion sont activés par défaut. Les opérations d'API de point de terminaison régional suivantes (opérations d'API au niveau du compartiment ou du plan de contrôle, opérations d'API) sont enregistrées. CloudTrail

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- PutBucketPolicy
- GetBucketPolicy
- ListDirectoryBuckets
- ListMultipartUploads
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

> **Note**
>
> `ListMultipartUploads` est une opération d'API de point de terminaison zonal. Cependant, il est enregistré en CloudTrail tant qu'événement de gestion. Pour plus d'informations, consultez ListMultipartUploads dans la Référence d'API Amazon Simple Storage Service.

Par défaut, les CloudTrail sentiers n'enregistrent pas les événements de données, mais vous pouvez configurer les sentiers pour qu'ils enregistrent les événements de données pour les compartiments de répertoire que vous spécifiez ou pour enregistrer les événements de données pour tous les compartiments de répertoire de votre AWS compte. Les opérations d'API de point de terminaison zonales suivantes (opérations d'API au niveau de l'objet ou du plan de données, opérations d'API) sont enregistrées. CloudTrail

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateSession
- CopyObject
- CreateMultipartUpload
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

Pour plus d'informations sur l'utilisation AWS CloudTrail des compartiments de répertoire, consultez la section Logging with AWS CloudTrail pour les compartiments de répertoire.

Mettre en œuvre la surveillance à l'aide d'outils AWS de surveillance

La surveillance joue un rôle important dans le maintien de la fiabilité, de la sécurité, de la disponibilité et des performances d'Amazon S3 et de vos AWS solutions. AWS fournit plusieurs outils et services pour vous aider à surveiller Amazon S3 et vos autres Services AWS. Par exemple, vous pouvez surveiller CloudWatch les métriques Amazon pour Amazon S3, en particulier les métriques `NumberOfObjects` de stockage `BucketSizeBytes` et.

Les objets stockés dans les compartiments de répertoires ne seront pas reflétés dans les métriques de stockage `BucketSizeBytes` et `NumberOfObjects` d'Amazon S3. Toutefois, les métriques de stockage `BucketSizeBytes` et `NumberOfObjects` sont prises en charge pour les compartiments de répertoires. Pour consulter les métriques de votre choix, vous pouvez différencier les classes de stockage Amazon S3 en spécifiant une dimension `StorageType`. Pour de plus amples informations, veuillez consulter Surveillance des métriques avec Amazon CloudWatch.

Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch et Journalisation et surveillance dans Amazon S3.

Gestion de l'accès aux ensembles de données partagés dans des compartiments d'annuaire dotés de points d'accès

Les points d'accès Amazon S3 simplifient la gestion de l'accès aux données à grande échelle pour les ensembles de données partagés dans Amazon S3. Les points d'accès sont des noms d'hôtes uniques que vous créez pour appliquer des autorisations et des contrôles réseau distincts pour toutes les demandes effectuées via un point d'accès. Vous pouvez créer des centaines de points d'accès par compartiment, chacun portant un nom distinct et des autorisations personnalisées pour chaque application. Chaque point d'accès fonctionne conjointement avec la politique de compartiment attachée au compartiment sous-jacent.

Dans les compartiments d'annuaire, le nom d'un point d'accès se compose du nom de base que vous fournissez, suivi de l'ID de zone (zone de AWS disponibilité ou zone locale) de l'emplacement de votre compartiment de répertoire, puis`--xa-s3`. Par exemple, *`accesspointname`*`--`*`zoneID`*`--xa-s3`. Une fois que vous avez créé un point d'accès, vous ne pouvez pas modifier le nom ou l'ID de zone.

Avec les points d'accès pour les compartiments de répertoires, vous pouvez utiliser l'étendue du point d'accès pour restreindre l'accès à des préfixes ou à des opérations d'API spécifiques. Vous pouvez spécifier n'importe quel nombre de préfixes, mais la longueur totale des caractères de tous les préfixes doit être inférieure à 256 octets.

Vous pouvez configurer n'importe quel point d'accès pour accepter uniquement les demandes provenant d'un cloud privé virtuel (VPC). Cela limite l'accès aux données Amazon S3 à un réseau privé.

Dans cette section, les rubriques expliquent comment utiliser les points d'accès pour les compartiments d'annuaire. Pour plus d'informations sur les compartiments de répertoire, consultezUtilisation des compartiments de répertoires.

Rubriques

- Points d'accès pour les règles de dénomination, restrictions et limitations des compartiments de répertoire
- Référencement des points d'accès pour les compartiments de répertoire
- Opérations sur les objets pour les points d'accès aux compartiments de répertoire
- Configuration des politiques IAM pour l'utilisation des points d'accès pour les compartiments d'annuaire
- Surveillance et journalisation des points d'accès pour les compartiments d'annuaire
- Création de points d'accès pour les compartiments de répertoires
- Gestion de vos points d'accès pour les buckets d'annuaires
- Utilisation de balises avec des points d'accès S3 pour les compartiments de répertoire

Points d'accès pour les règles de dénomination, restrictions et limitations des compartiments de répertoire

Les points d'accès simplifient la gestion de l'accès aux données à grande échelle pour les ensembles de données partagés dans Amazon S3. Les rubriques suivantes fournissent des informations sur les règles de dénomination des points d'accès, ainsi que sur les restrictions et limitations.

Rubriques

- Règles de dénomination des points d'accès pour les compartiments de répertoire
- Restrictions et limitations relatives aux points d'accès pour les compartiments de répertoire

Règles de dénomination des points d'accès pour les compartiments de répertoire

Un point d'accès doit être créé dans la même zone que celle dans laquelle se trouve le bucket. Le nom du point d'accès doit être unique dans la zone.

Les noms des points d'accès doivent être conformes au DNS et répondre aux conditions suivantes :

- Ils doivent commencer par un chiffre ou une lettre minuscule.

- Le nom de base que vous fournissez doit comporter entre 3 et 50 caractères
- Ils ne peuvent pas commencer ou se terminer par un trait d'union (-)
- Ne peut pas contenir de traits de soulignement (_), de lettres majuscules, d'espaces ou de points (.)
- Doit se terminer par le suffixe*zoneid*--xa--s3.

Restrictions et limitations relatives aux points d'accès pour les compartiments de répertoire

Les points d'accès pour les compartiments de répertoire sont soumis aux restrictions et limitations suivantes :

- Chaque point d'accès est associé à un compartiment de répertoire. Une fois que vous avez créé un point d'accès, vous ne pouvez pas l'associer à un autre bucket. Toutefois, vous pouvez supprimer un point d'accès, puis en créer un nouveau portant le même nom et l'associer à un autre bucket.
- Après avoir créé un point d'accès, vous ne pouvez pas modifier sa configuration VPC (virtual private cloud).
- Les stratégies de point d'accès sont limitées à une taille de 20 Ko.
- Les préfixes d'étendue des points d'accès sont limités à 256 octets au total.
- Vous pouvez créer un maximum de 10 000 points d'accès Compte AWS par personne Région AWS. Si vous avez besoin de plus de 10 000 points d'accès pour un seul compte dans une même région, vous pouvez demander une augmentation des quotas de service. Pour plus d'informations sur les quotas de service et la demande d'une augmentation, consultez AWS Service Quotas dans Références générales AWS.
- Vous ne pouvez utiliser que des points d'accès pour effectuer des opérations sur des objets. Vous ne pouvez pas utiliser les points d'accès pour effectuer des opérations sur les compartiments Amazon S3, telles que la modification ou la suppression de compartiments. Pour obtenir la liste complète des opérations prises en charge, consultezOpérations sur les objets pour les points d'accès aux compartiments de répertoire.
- Vous pouvez faire référence aux points d'accès par leur nom, leur alias ou leur virtual-hosted-style URI. Vous ne pouvez pas adresser les points d'accès par ARN. Pour de plus amples informations, veuillez consulter Référencement des points d'accès pour les compartiments de répertoire.
- Les opérations d'API qui contrôlent les fonctionnalités du point d'accès (par exemple, `PutAccessPointPolicy` et`GetAccessPointPolicy`) doivent spécifier le AWS compte propriétaire du point d'accès.

- Vous devez utiliser AWS Signature Version 4 lorsque vous envoyez des demandes à un point d'accès à l'aide de l'API REST. Pour plus d'informations sur l'authentification des demandes, consultez Authentification des demandes (AWS Signature version 4) dans le manuel Amazon Simple Storage Service API Reference.
- Les points d'accès prennent uniquement en charge les demandes via HTTPS. Amazon S3 répondra automatiquement par une redirection HTTP pour toutes les demandes effectuées via HTTP, afin de passer à HTTPS.
- Les points d'accès ne prennent pas en charge l'accès anonyme.
- Si vous créez un point d'accès à un bucket appartenant à un autre compte (point d'accès multi-comptes), le point d'accès inter-comptes ne vous accorde pas l'accès aux données tant que le propriétaire du bucket ne vous autorise pas à accéder au bucket. Le propriétaire du compartiment conserve toujours le contrôle ultime sur l'accès aux données et doit mettre à jour la politique du compartiment pour autoriser les demandes provenant du point d'accès intercompte. Pour afficher un exemple de politique de compartiment, consultez Configuration des politiques IAM pour l'utilisation des points d'accès pour les compartiments d'annuaire.

Référencement des points d'accès pour les compartiments de répertoire

Après avoir créé un point d'accès, vous pouvez l'utiliser comme point de terminaison pour effectuer des opérations sur des objets. Pour les points d'accès pour les compartiments de répertoire, l'alias du point d'accès est identique au nom du point d'accès. Vous pouvez utiliser le nom du point d'accès au lieu d'un nom de compartiment pour toutes les opérations de données. Pour obtenir la liste de ces opérations prises en charge, consultezOpérations sur les objets pour les points d'accès aux compartiments de répertoire.

En faisant référence aux points d'accès par virtual-hosted-style URIs

Les points d'accès prennent uniquement en charge l' virtual-host-styleadressage. Les points d'accès utilisent le même format que les points de terminaison des compartiments de répertoire. Pour de plus amples informations, veuillez consulter Points de terminaison d'API régionaux et zonaux des compartiments de répertoires.

Les points d'accès S3 ne prennent pas en charge l'accès via HTTP. Les points d'accès prennent uniquement en charge l'accès sécurisé par HTTPS.

Opérations sur les objets pour les points d'accès aux compartiments de répertoire

Vous pouvez utiliser des points d'accès pour accéder à un objet à l'aide S3 des opérations de données suivantes.

- AbortMultipartUpload
- CompleteMultipartUpload
- CopyObject
- CreateMultipartUpload
- CreateSession
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- UploadPart
- UploadPartCopy

Configuration des politiques IAM pour l'utilisation des points d'accès pour les compartiments d'annuaire

Politiques de ressources de support des points d'accès AWS Identity and Access Management (IAM) qui vous permettent de contrôler l'utilisation du point d'accès par ressource, par utilisateur ou selon d'autres conditions. Pour qu'une application ou un utilisateur puisse accéder à des objets via un point d'accès, le point d'accès et la politique de compartiment sous-jacente doivent autoriser la demande.

> **Important**
>
> L'ajout d'un point d'accès à un bucket de répertoire ne modifie pas le comportement du bucket lorsque le bucket est accessible directement via le nom du bucket. Toutes les opérations existantes sur le compartiment continueront de fonctionner comme auparavant. Les restrictions que vous incluez dans une politique de point d'accès ou dans l'étendue d'un point d'accès ne s'appliquent qu'aux demandes effectuées via ce point d'accès.

Lorsque vous utilisez des politiques de ressources IAM, veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions AWS Identity and Access Management Access Analyzer avant d'enregistrer votre politique. IAM Access Analyzer exécute des vérifications de politiques pour valider votre politique par rapport à la grammaire de politique et aux bonnes pratiques IAM. Ces vérifications génèrent des résultats et fournissent des recommandations pour vous aider à créer des stratégies fonctionnelles et conformes aux bonnes pratiques en matière de sécurité.

Pour en savoir plus sur la validation des politiques à l'aide d'IAM Access Analyzer, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM. Pour afficher la liste des avertissements, erreurs et suggestions renvoyés par IAM Access Analyzer, consultez la Référence de vérification de politique IAM Access Analyzer.

Exemples de politiques relatives aux points d'accès pour les compartiments d'annuaire

Les politiques de point d'accès suivantes montrent comment contrôler les demandes adressées à un bucket d'annuaire. Les politiques relatives aux points d'accès nécessitent un compartiment ARNs ou un point d'accès ARNs. Les alias de point d'accès ne sont pas pris en charge dans les politiques. Voici un exemple d'ARN de point d'accès :

```
arn:aws:s3express:region:account-id:accesspoint/myaccesspoint--zoneID--xa-s3
```

Vous pouvez consulter l'ARN du point d'accès dans les détails d'un point d'accès. Pour de plus amples informations, veuillez consulter Afficher les détails de vos points d'accès pour les compartiments d'annuaire.

> **Note**
>
> Les autorisations accordées dans une politique de point d'accès ne sont effectives que si le compartiment sous-jacent autorise également le même accès. Vous pouvez y parvenir de deux façons :
>
> 1. (Recommandé) Déléguer le contrôle d'accès du compartiment au point d'accès, comme décrit à la section Délégation du contrôle d'accès aux points d'accès.
> 2. Ajoutez les mêmes autorisations contenues dans la stratégie de point d'accès à la stratégie du compartiment sous-jacent.

Example 1 — Politique de contrôle des services pour limiter les points d'accès aux origines du réseau VPC

La politique de contrôle des services suivante exige que tous les nouveaux points d'accès soient créés à partir d'un réseau de cloud privé virtuel (VPC). Avec cette politique en place, les utilisateurs de votre organisation ne peuvent créer aucun point d'accès accessible depuis Internet.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3express:CreateAccessPoint",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3express:AccessPointNetworkOrigin": "VPC"
            }
        }
    }
  ]
}
```

Example 2 — Politique de point d'accès pour limiter l'accès au bucket aux points d'accès provenant d'un réseau VPC

La politique de point d'accès suivante limite tous les accès au bucket *amzn-s3-demo-bucket--zoneID--x-s3* à un point d'accès ayant une origine réseau VPC.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyCreateSessionFromNonVPC",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "Effect": "Deny",
            "Resource": "arn:aws:s3express:us-east-1:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3"
        }
    ]
}
```

Clés de condition

Les points d'accès pour les compartiments d'annuaire sont dotés de clés de condition que vous pouvez utiliser dans les politiques IAM pour contrôler l'accès à vos ressources. Les clés de condition suivantes ne représentent qu'une partie d'une politique IAM. Pour obtenir des exemples complets de politiques, consultez Exemples de politiques relatives aux points d'accès pour les compartiments d'annuaire, Délégation du contrôle d'accès aux points d'accès et Octroi d'autorisations pour les points d'accès intercompte.

`s3express:DataAccessPointArn`

Cet exemple montre comment filtrer l'accès en fonction du nom de ressource Amazon (ARN) d'un point d'accès et fait correspondre tous les points d'accès Compte AWS *111122223333* de la région *region* :

```
"Condition" : {
    "StringLike": {
```

```
        "s3express:DataAccessPointArn":
 "arn:aws:s3express:region:111122223333:accesspoint/*"
    }
}
```

s3express:DataAccessPointAccount

Cet exemple présente un opérateur de chaîne que vous pouvez utiliser pour établir une correspondance sur l'ID de compte du propriétaire d'un point d'accès. L'exemple suivant correspond à tous les points d'accès appartenant au Compte AWS *111122223333*.

```
"Condition" : {
    "StringEquals": {
        "s3express:DataAccessPointAccount": "111122223333"
    }
}
```

s3express:AccessPointNetworkOrigin

Cet exemple présente un opérateur de chaîne que vous pouvez utiliser pour faire correspondre sur l'origine du réseau, soit `Internet`, soit VPC. L'exemple suivant ne correspond qu'aux points d'accès ayant une origine VPC.

```
"Condition" : {
    "StringEquals": {
        "s3express:AccessPointNetworkOrigin": "VPC"
    }
}
```

s3express:Permissions

Vous pouvez l'utiliser `s3express:Permissions` pour restreindre l'accès à des opérations d'API spécifiques dans le périmètre du point d'accès. Les opérations d'API suivantes sont prises en charge :

- `PutObject`
- `GetObject`
- `DeleteObject`
- `ListBucket`(obligatoire pour`ListObjectsV2`)
- `GetObjectAttributes`

- `AbortMultipartUpload`
- `ListBucketMultipartUploads`
- `ListMultipartUploadParts`

> **Note**
>
> Lorsque vous utilisez des clés de condition à valeurs multiples, nous vous recommandons de les utiliser `ForAllValues` avec `Allow` des instructions et `ForAnyValue` avec des `Deny` instructions. Pour plus d'informations, consultez la section Clés contextuelles à valeurs multiples dans le guide de l'utilisateur IAM.

Pour plus d'informations sur l'utilisation des clés de condition avec Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations requises pour les opérations d'API S3 par type de ressource S3, consultezAutorisations requises pour les opérations d'API Amazon S3.

Délégation du contrôle d'accès aux points d'accès

Vous pouvez déléguer le contrôle d'accès de la politique de compartiment à la politique de point d'accès. Dans l'exemple suivant, la politique de compartiment permet un accès complet à tous les points d'accès appartenant au compte du propriétaire du compartiment. Une fois la politique appliquée, tous les accès à ce compartiment sont contrôlés par des politiques de point d'accès. Nous vous recommandons de configurer vos compartiments de cette façon pour tous les cas d'utilisation qui ne demandent pas d'accès direct au compartiment.

Example politique de compartiment qui délègue le contrôle d'accès aux points d'accès

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "Bucket ARN",
        "Condition": {
            "StringEquals" : { "s3express:DataAccessPointAccount" : "Bucket owner's
 account ID" }
```

```
        }
    }]
}
```

Octroi d'autorisations pour les points d'accès intercompte

Pour créer un point d'accès à un compartiment qui appartient à un autre compte, vous devez d'abord créer le point d'accès en spécifiant le nom du compartiment et l'ID du propriétaire du compte. Ensuite, le propriétaire du compartiment doit mettre à jour la politique de compartiment pour autoriser les requêtes du point d'accès. La création d'un point d'accès est similaire à la création d'un DNS CNAME dans la mesure où le point d'accès ne donne pas accès au contenu du compartiment. Tous les accès aux compartiments sont contrôlés par la politique des compartiments. L'exemple de politique de compartiment suivant autorise les requêtes `GET` et `LIST` sur le compartiment depuis un point d'accès appartenant à un Compte AWS de confiance.

*`Bucket ARN`*Remplacez-le par l'ARN du bucket.

Example de la politique du bucket déléguant des autorisations à un autre Compte AWS

JSON

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Sid": "AllowCreateSessionForDirectoryBucket",
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "s3express:CreateSession",
        "Resource" : [ "arn:aws:s3express:us-west-2:111122223333:bucket/amzn-s3-demo-bucket--usw2-az1--x-s3" ],
        "Condition": {
            "ForAllValues:StringEquals": {
                "s3express:Permissions": [
                    "GetObject",
                    "ListBucket"
                ]
            }
        }
    }]
```

```
}
```

Surveillance et journalisation des points d'accès pour les compartiments d'annuaire

Vous pouvez enregistrer les demandes effectuées via les points d'accès et les demandes adressées aux points d'accès APIs qui gèrent les points d'accès, `GetAccessPointPolicy`, par exemple `CreateAccessPoint` et en utilisant AWS CloudTrail. CloudTrail les entrées du journal pour les demandes effectuées via les points d'accès incluent l'ARN du point d'accès (qui inclut le nom du point d'accès) dans la `resources` section du journal.

Par exemple, supposons que vous ayez la configuration suivante :

- Un compartiment nommé *amzn-s3-demo-bucket*`--`*zone-id*`--x-s3` dans Region `region` qui contient un objet nommé`my-image.jpg`.
- Un point d'accès nommé `my-bucket-ap--zoneID--xa-s3` associé à *amzn-s3-demo-bucket*`--`*zone-id*`--x-s3`
- Un Compte AWS identifiant de `123456789012`

L'exemple suivant montre la `resources` section d'une entrée de CloudTrail journal pour la configuration précédente :

```
"resources": [
        {"type": "AWS::S3Express::Object",

            "ARN": "arn:aws:s3express-region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3/my-image.jpg"
        },
        {"accountId": "c",
            "type": "AWS::S3Express::DirectoryBucket",
            "ARN": "arn:aws::s3express:region:123456789012:bucket/amzn-s3-demo-
bucket--zone-id--x-s3"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::AccessPoint",
            "ARN": "arn:aws:s3express:region:123456789012:accesspoint/my-bucket-ap--
zoneID--xa-s3"
        }
```

```
]
```

Pour plus d'informations AWS CloudTrail, voir Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

Création de points d'accès pour les compartiments de répertoires

À l'instar des buckets d'annuaire, les points d'accès peuvent être créés dans des zones de disponibilité ou dans des zones locales dédiées. Le point d'accès doit être créé dans la même zone que le bucket de répertoire qui lui est associé.

Un point d'accès est associé à un seul compartiment d'annuaire Amazon S3. Si vous souhaitez utiliser un compartiment de répertoire dans votre répertoire Compte AWS, vous devez d'abord créer un compartiment de répertoire. Pour plus d'informations sur la création de compartiments de répertoires, consultez Création de compartiments de répertoires dans une zone de disponibilité ouCréation d'un compartiment de répertoires dans une zone locale.

Vous pouvez également créer un point d'accès intercompte associé à un compartiment dans un autre compte Compte AWS, à condition de connaître le nom du compartiment et l'ID du compte du propriétaire du compartiment. Cependant, la création de points d'accès intercompte ne vous donne pas accès aux données du compartiment tant que vous n'avez pas obtenu les autorisations du propriétaire du compartiment. Le propriétaire du compartiment doit accorder au compte du propriétaire du point d'accès (votre compte) l'accès au compartiment par le biais de la stratégie du compartiment. Pour de plus amples informations, veuillez consulter Octroi d'autorisations pour les points d'accès intercompte.

Vous pouvez créer un point d'accès pour n'importe quel compartiment de répertoire à l' AWS Management Console aide de l'API REST, ou AWS SDKs. AWS CLI Chaque point d'accès est associé à un seul compartiment de répertoire, et vous pouvez créer des centaines de points d'accès par compartiment. Lorsque vous créez un point d'accès, vous choisissez le nom du point d'accès et le compartiment de répertoire auquel l'associer. Le nom du point d'accès se compose d'un nom de base que vous fournissez et d'un suffixe qui inclut l'ID de zone de l'emplacement de votre compartiment, suivi `--xa-s3` de. Par exemple, *`myaccesspoint-zoneID`*`--xa-s3` vous pouvez également restreindre l'accès au point d'accès via un Virtual Private Cloud (VPC). Ensuite, vous pouvez immédiatement commencer à lire et à écrire des données via votre point d'accès en utilisant son nom, comme vous utilisez le nom d'un bucket de répertoire.

Vous pouvez utiliser l'étendue du point d'accès pour restreindre l'accès au compartiment de répertoire via le point d'accès à des préfixes ou à des opérations d'API spécifiques. Si vous n'ajoutez

pas d'étendue au point d'accès, tous les préfixes du compartiment de répertoire et toutes les opérations d'API peuvent être effectués sur les objets du compartiment lorsqu'ils sont accessibles via le point d'accès. Après avoir créé le point d'accès, vous pouvez ajouter, modifier ou supprimer une étendue à l'aide de l'API AWS CLI AWS SDKs, ou de l'API REST. Pour de plus amples informations, veuillez consulter Gérez l'étendue de vos points d'accès pour les compartiments d'annuaire.

Après avoir créé le point d'accès, vous pouvez configurer la politique de ressources IAM de votre point d'accès. Pour de plus amples informations, veuillez consulter Afficher, modifier ou supprimer les politiques relatives aux points d'accès.

Utilisation de la console S3

> **Note**
>
> Vous pouvez également créer un point d'accès pour un compartiment de répertoire à partir de l'écran du compartiment de répertoire. Dans ce cas, le nom du compartiment de répertoire est fourni et il n'est pas nécessaire de choisir un compartiment lors de la création du point d'accès. Pour de plus amples informations, veuillez consulter Établissement de la liste des compartiments de répertoires.

Pour créer un point d'accès pour les compartiments de répertoire

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un point d'accès. Le point d'accès doit être créé dans la même région que le bucket associé.
3. Dans le volet de navigation de gauche, choisissez Access points for directory buckets.
4. Dans la page Points d'accès, choisissez Créer un point d'accès.
5. Vous pouvez créer un point d'accès pour un bucket de répertoire dans votre compte ou dans un autre compte. Pour créer un point d'accès pour un bucket de répertoire dans un autre compte, procédez comme suit :

   > **Note**
   >
   > Si vous utilisez un bucket dans un autre endroit Compte AWS, le propriétaire du bucket doit mettre à jour la politique du bucket afin d'autoriser les demandes provenant du point

d'accès. Pour un exemple de politique de compartiment, consultez Octroi d'autorisations pour les points d'accès intercompte.

a. Dans le champ Directory bucket, choisissez Spécifier un bucket dans un autre compte.

b. Dans le champ ID de compte du propriétaire du compartiment, entrez l' Compte AWS identifiant du propriétaire du compartiment.

c. Dans le champ Nom du compartiment, entrez le nom du compartiment, y compris le nom de base et l'ID de zone. Par exemple, ***bucket-base-name*--*zone-id*--x-s3**.

6. Pour créer un point d'accès pour un bucket de répertoire dans votre compte, procédez comme suit :

a. Dans le champ Directory bucket, choisissez Choose a bucket in this account.

b. Dans le champ Nom du compartiment, entrez le nom du compartiment, y compris le nom de base et l'ID de zone. Par exemple, ***bucket-base-name*--*zone-id*--x-s3**. Pour choisir le bucket dans une liste, choisissez Browse S3 et choisissez le bucket de répertoire.

7. Dans Nom du point d'accès, dans le champ Nom de base, entrez le nom de base du point d'accès. L'ID de zone et le nom complet du point d'accès apparaissent. Pour en savoir plus sur l'attribution de noms aux points d'accès, consultez Règles de dénomination des points d'accès pour les compartiments de répertoire.

8. Dans Origine du réseau, choisissez le cloud privé virtuel (VPC) ou Internet. Si vous choisissez le cloud privé virtuel (VPC), dans le champ ID VPC, entrez l'ID du VPC que vous souhaitez utiliser avec le point d'accès.

9. (Facultatif) Dans Zone d'étendue du point d'accès, pour appliquer une étendue à ce point d'accès, choisissez Limiter la portée de ce point d'accès à l'aide de préfixes ou d'autorisations.

a. Pour limiter l'accès aux préfixes du compartiment de répertoire, dans Préfixes, entrez un ou plusieurs préfixes. Pour ajouter un autre préfixe, choisissez Ajouter un préfixe. Pour supprimer un préfixe, choisissez Supprimer.

> **Note**
>
> Le champ d'application d'un point d'accès est limité à 512 caractères au total pour tous les préfixes. Vous pouvez voir le nombre de caractères restant sous Ajouter un préfixe.

b. Dans Autorisations, choisissez une ou plusieurs opérations d'API que le point d'accès autorisera. Pour supprimer une opération de données, choisissez le X à côté du nom de l'opération de données.

10. Pour ne pas appliquer d'étendue au point d'accès et autoriser l'accès à tous les préfixes du compartiment de répertoire et à toutes les opérations d'API via le point d'accès, dans Portée du point d'accès, choisissez Appliquer l'accès à l'ensemble du compartiment.
11. Choisissez Create access point for directory bucket. Le nom du point d'accès et d'autres informations le concernant apparaissent dans la liste des points d'accès pour les compartiments d'annuaire.

À l'aide du AWS CLI

L'exemple de commande suivant crée un point d'accès nommé *example-ap* pour le compartiment *amzn-s3-demo-bucket--zone-id--x-s3* dans le compte *111122223333*.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3
```

Pour restreindre l'accès au point d'accès via un VPC, incluez le `--vpc` paramètre et l'ID du VPC.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --vpc vpc-id
```

Lorsque vous créez un point d'accès pour un bucket multi-comptes, incluez le `--bucket-account-id` paramètre. L'exemple de commande suivant crée un point d'accès dans le Compte AWS *111122223333*, pour le compartiment*amzn-s3-demo-bucket--zone-id--x-s3*, appartenant au Compte AWS *444455556666*.

```
aws s3control create-access-point --name example-ap--zoneID--xa-s3 --account-
id 111122223333 --bucket amzn-s3-demo-bucket--zone-id--x-s3 --bucket-account-
id 444455556666
```

Pour plus d'informations et des exemples, reportez-vous create-access-pointà la référence des AWS CLI commandes.

Utilisation de l'API REST

L'exemple de commande suivant crée un point d'accès nommé *example-ap* d'après le bucket *amzn-s3-demo-bucket--zone-id--x-s3* du compte *111122223333* et l'accès est restreint via le VPC *vpc-id* (facultatif).

```
PUT /v20180820/accesspoint/example-ap--zoneID--xa-s3 HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointRequest>
   <Bucket>amzn-s3-demo-bucket--zone-id--x-s3s</Bucket>
   <BucketAccountId>111122223333</BucketAccountId>
   <VpcConfiguration>
       <VpcId>vpc-id</VpcId>
   </VpcConfiguration>
</CreateAccessPointRequest>
```

Réponse :

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<CreateAccessPointResult>
   <AccessPointArn>
       "arn:aws:s3express:region:111122223333:accesspoint/example-ap--zoneID--xa-s3"
   </AccessPointArn>
   <Alias>example-ap--zoneID--xa-s3</Alias>
</CreateAccessPointResult>
```

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour créer un point d'accès. Pour plus d'informations, consultez la liste des produits pris SDKs en charge dans le manuel Amazon Simple Storage Service API Reference.

Gestion de vos points d'accès pour les buckets d'annuaires

Cette section explique comment gérer vos points d'accès pour les compartiments de répertoire à l'aide de l' AWS Command Line Interface API REST ou du AWS SDK Amazon S3.

Rubriques

- Répertoriez vos points d'accès pour les buckets de répertoires
- Afficher les détails de vos points d'accès pour les compartiments d'annuaire
- Afficher, modifier ou supprimer les politiques relatives aux points d'accès
- Gérez l'étendue de vos points d'accès pour les compartiments d'annuaire
- Supprimer votre point d'accès pour les compartiments de répertoire

Répertoriez vos points d'accès pour les buckets de répertoires

Cette section explique comment répertorier les points d'accès pour un bucket de répertoire à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI), REST ou AWS SDKs.

Utilisation de la console S3

Pour répertorier les points d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access points for directory buckets.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer.

À l'aide du AWS CLI

L'`list-access-points-for-directory-buckets`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour répertorier les points d'accès détenus par un AWS compte et associés à un bucket d'annuaire.

La commande suivante répertorie les points Compte AWS *111122223333* d'accès associés au bucket*amzn-s3-demo-bucket--zone-id--x-s3*.

```
aws s3control list-access-points-for-directory-buckets --account-id 111122223333 --
directory-bucket amzn-s3-demo-bucket--zone-id--x-s3
```

Pour plus d'informations et des exemples, consultez list-access-points-for-directory-buckets dans le manuel de référence des commandes. AWS CLI

Utilisation de l'API REST

L'exemple suivant montre comment utiliser l'API REST pour répertorier vos points d'accès.

```
GET /v20180820/directoryaccesspoint?directoryBucket=amzn-s3-demo-bucket--zone-id--x-s3
&maxResults=maxResults HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example de **`ListAccessPointsForDirectoryBuckets`** réponse

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<ListDirectoryAccessPointsResult>
    <AccessPointList>
        <AccessPoint>
            <AccessPointArn>arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3</AccessPointArn>
            <Alias>example-access-point--zoneID--xa-s3</Alias>
            <Bucket>amzn-s3-demo-bucket--zone-id--x-s3</Bucket>
            <BucketAccountId>111122223333</BucketAccountId>
            <Name>example-access-point--zoneID--xa-s3</Name>
            <NetworkOrigin>VPC</NetworkOrigin>
```

```
            <VpcConfiguration>
                <VpcId>VPC-1</VpcId>
            </VpcConfiguration>
        </AccessPoint>
    </AccessPointList>
</ListDirectoryAccessPointsResult>
```

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour répertorier vos points d'accès. Pour plus d'informations, consultez la liste des produits pris SDKs en charge dans le manuel Amazon Simple Storage Service API Reference.

Afficher les détails de vos points d'accès pour les compartiments d'annuaire

Cette section explique comment afficher les détails de votre point d'accès pour les compartiments de répertoire à l'aide de l'API AWS Management Console AWS CLI, AWS SDKs, ou REST.

Utilisation de la console S3

Consultez les détails d'un point d'accès pour les compartiments de répertoire afin de consulter les informations suivantes sur le point d'accès et le compartiment de répertoire associé :

- Propriétés
  - Nom du bucket du répertoire
  - ID de compte du propriétaire du bucket d'annuaire
  - Région AWS
  - Type d'emplacement du compartiment de répertoire
  - Nom de l'emplacement du compartiment de répertoire
  - Date de création du point d'accès
  - Origine du réseau
  - VPC ID
  - URI S3
  - ARN de point d'accès
  - Alias du point d'accès
- Autorisations :

- Résultats de l'analyseur d'accès externe IAM
- Portée du point d'accès
- Politique relative aux points d'accès

Pour consulter les détails de votre point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access points for directory buckets.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer.
6. Choisissez l'onglet Propriétés ou l'onglet Autorisations.

À l'aide du AWS CLI

L'`get-access-point`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour afficher les détails de votre point d'accès.

La commande suivante répertorie les détails du point d'accès *my-access-point--zoneID--xa-s3* pour Compte AWS *111122223333*.

```
aws s3control get-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Example de sortie de **`get-access-point`** commande

```
{
    "Name": "example-access-point--zoneID--xa-s3",
    "Bucket": "amzn-s3-demo-bucket--zone-id--x-s3",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
```

```
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2025-04-23T18:26:22.146000+00:00",
    "Alias": "example-access-point--zoneID--xa-s3",
    "AccessPointArn": "arn:aws:s3express:region:111122223333:accesspoint/example-
access-point--zoneID--xa-s3",
    "BucketAccountId": "296805379465"
}
```

Pour plus d'informations et des exemples, consultez get-access-point dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour afficher les détails de votre point d'accès. Pour plus d'informations, consultez GetAccessPoint dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour afficher les détails de vos points d'accès. Pour plus d'informations, consultez la liste des produits pris SDKs en charge dans le manuel Amazon Simple Storage Service API Reference.

Afficher, modifier ou supprimer les politiques relatives aux points d'accès

Vous pouvez utiliser une politique de point d'accès AWS Identity and Access Management (IAM) pour contrôler le principal et la ressource autorisés à accéder au point d'accès. L'étendue du point d'accès gère les préfixes et les autorisations d'API pour le point d'accès. Vous pouvez créer, modifier et supprimer une politique de point d'accès à l' AWS Command Line Interface aide de l'API REST ou AWS SDKs. Pour plus d'informations sur l'étendue du point d'accès, consultezGérez l'étendue de vos points d'accès pour les compartiments d'annuaire.

> **Note**
>
> Étant donné que les compartiments d'annuaire utilisent l'autorisation basée sur les sessions, votre politique doit toujours inclure l'action. `s3express:CreateSession`

Utilisation de la console S3

Pour consulter, modifier ou supprimer une politique de point d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access points for directory buckets.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer.
6. Sélectionnez l'onglet Autorisations.
7. Pour créer ou modifier la politique de point d'accès, dans Politique de point d'accès, choisissez Modifier. Modifiez la politique. Choisissez Enregistrer.
8. Pour supprimer la politique de point d'accès, dans Politique de point d'accès, choisissez Supprimer. Dans la fenêtre Supprimer la politique de point d'accès, tapez **`confirm`** et choisissez Supprimer.

En utilisant le AWS CLI

Vous pouvez utiliser les `delete-access-point-policy` commandes `get-acccess-point-policyput-access-point-policy`, et pour afficher, modifier ou supprimer une politique de point d'accès. Pour plus d'informations, consultez get-access-point-policyput-access-point-policy, ou delete-access-point-policydans le manuel de référence des AWS CLI commandes.

Utilisation de l'API REST

Vous pouvez utiliser l'API REST `GetAccessPointPolicy` et les `PutAccessPointPolicy` opérations pour afficher, supprimer ou modifier une politique de point d'accès. `DeleteAccessPointPolicy` Pour plus d'informations PutAccessPointPolicyGetAccessPointPolicy, consultez ou consultez le DeleteAccessPointPolicymanuel Amazon Simple Storage Service API Reference.

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour afficher, supprimer ou modifier une politique de point d'accès. Pour plus d'informations, consultez la liste des produits pris en charge SDKs pour GetAccessControlPolicyet PutAccessControlPolicydans le manuel Amazon Simple Storage Service API Reference. DeleteAccessControlPolicy

Gérez l'étendue de vos points d'accès pour les compartiments d'annuaire

Cette section explique comment afficher et modifier l'étendue de vos points d'accès pour les compartiments de répertoire à l'aide de l' AWS Command Line Interface API REST ou AWS SDKs. Vous pouvez utiliser l'étendue du point d'accès pour restreindre l'accès à des préfixes ou à des opérations d'API spécifiques.

Rubriques

- Afficher l'étendue de vos points d'accès pour les buckets d'annuaire
- Modifier l'étendue de votre point d'accès pour les buckets d'annuaire
- Supprimez l'étendue de vos points d'accès pour les compartiments d'annuaire

Afficher l'étendue de vos points d'accès pour les buckets d'annuaire

Vous pouvez utiliser l'API REST AWS Management Console AWS Command Line Interface, ou AWS SDKs pour afficher l'étendue de votre point d'accès pour les buckets de répertoires.

Utilisation de la console S3

Pour afficher l'étendue de votre point d'accès pour les buckets d'annuaire

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access points for directory buckets.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.

5. Choisissez le nom du point d'accès que vous souhaitez gérer.
6. Sélectionnez l'onglet Autorisations.
7. Dans le champ d'application du point d'accès, vous pouvez voir les préfixes et les autorisations appliqués au point d'accès.

En utilisant le AWS CLI

L'`get-access-point-scope`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour afficher l'étendue de votre point d'accès.

La commande suivante montre l'étendue du point d'accès *`my-access-point`* -- *`zoneID`* --xa-s3 for. Compte AWS *`111122223333`*

```
aws s3control get-access-point-scope --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Pour plus d'informations et des exemples, reportez-vous get-access-point-scopeà la référence des AWS CLI commandes.

Example résultat de **`get-access-point-scope`**

```
{
    "Scope": {
        "Permissions": [
            "ListBucket",
            "PutObject"
        ]
  "Prefixes": [
            "Prefix": "MyPrefix1*",
            "Prefix": "MyObjectName.csv"
        ]
    }
}
```

Utilisation de l'API REST

L'`GetAccessPointScope`exemple de demande suivant montre comment vous pouvez utiliser l'API REST pour afficher l'étendue de votre point d'accès.

La requête suivante indique l'étendue du point d'accès *my-access-point* -- *region* - *zoneID* --xa-s3 pour. Compte AWS *111122223333*

```
GET /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

Example résultat de **GetAccessPointScope**

```
HTTP/1.1 200
<?xml version="1.0" encoding="UTF-8"?>
<GetAccessPointScopeResult>
    <Scope>
        <Prefixes>
            <Prefix>MyPrefix1*</Prefix>
            <Prefix>MyObjectName.csv</Prefix>
        </Prefixes>
        <Permissions>
            <Permission>ListBucket</Permission>
            <Permission>PutObject</Permission>
        </Permissions>
        <Scope>
</GetAccessPointScopeResult>
```

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour afficher l'étendue de votre point d'accès. Pour plus d'informations, consultez la liste des produits pris SDKs en charge dans le manuel Amazon Simple Storage Service API Reference.

Modifier l'étendue de votre point d'accès pour les buckets d'annuaire

Vous pouvez utiliser l'API REST AWS Management Console AWS Command Line Interface, ou AWS SDKs pour modifier l'étendue de vos points d'accès pour les buckets de répertoires. L'étendue du point d'accès est utilisée pour restreindre l'accès à des préfixes spécifiques, à des opérations d'API ou à une combinaison des deux.

Vous pouvez inclure une ou plusieurs des opérations d'API suivantes en tant qu'autorisations :

- `PutObject`
- `GetObject`
- `DeleteObject`
- `ListBucket`(obligatoire pour`ListObjectsV2`)
- `GetObjectAttributes`
- `AbortMultipartUploads`
- `ListBucketMultipartUploads`
- `ListMultipartUploadParts`

> **Note**
>
> Vous pouvez spécifier n'importe quel nombre de préfixes, mais la longueur totale des caractères de tous les préfixes doit être inférieure à 256 octets.

Utilisation de la console S3

Pour modifier l'étendue du point d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access points for directory buckets.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer.
6. Sélectionnez l'onglet Autorisations.
7. Dans la section Portée du point d'accès, choisissez Modifier.
8. Pour ajouter ou supprimer des préfixes :

a. Pour ajouter un préfixe, choisissez Ajouter un préfixe. Dans le champ Préfixe, entrez le préfixe du compartiment de répertoire. Répétez l'opération pour ajouter d'autres préfixes.

b. Pour supprimer un préfixe, choisissez Supprimer.

9. Pour ajouter ou supprimer des autorisations, procédez comme suit :

a. Pour ajouter une autorisation, dans le champ Choisir les opérations de données, sélectionnez l'autorisation.

b. Pour supprimer une autorisation, cliquez sur le X à côté de l'autorisation.

10. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

L'`put-access-point-scope`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour modifier l'étendue de votre point d'accès.

La commande suivante modifie l'étendue du point d'accès de *`my-access-point`* -- *`zoneID`* --xa-s3 for. Compte AWS *`111122223333`*

> **Note**
>
> Vous pouvez utiliser des caractères génériques dans les préfixes en utilisant l'astérisque (*). Si vous souhaitez utiliser l'astérisque comme littéral, ajoutez une barre oblique inverse (\) avant celui-ci pour y échapper.
> Tous les préfixes ont une terminaison implicite « * », ce qui signifie que tous les chemins compris dans le préfixe seront inclus.
> Lorsque vous modifiez l'étendue d'un point d'accès par le AWS CLI, vous remplacez l'étendue existante.

```
aws s3control put-access-point-scope --name my-access-point--zoneID--xa-s3 --account-
id 111122223333 --scope Prefixes=string,Permissions=string
```

Pour plus d'informations et des exemples, reportez-vous put-access-point-scopeà la référence des AWS CLI commandes.

Utilisation de l'API REST

L'`PutAccessPointScope`exemple de demande suivant montre comment vous pouvez utiliser l'API REST pour modifier l'étendue de votre point d'accès.

La requête suivante modifie l'étendue du point d'accès de *`my-access-point`* -- *`zoneID`* --xa-s3 for. Compte AWS *`111122223333`*

> **Note**
>
> Vous pouvez utiliser des caractères génériques dans les préfixes en utilisant l'astérisque (*). Si vous souhaitez utiliser l'astérisque comme littéral, ajoutez une barre oblique inverse (\) avant celui-ci pour y échapper.
> Tous les préfixes ont une terminaison implicite « * », ce qui signifie que tous les chemins compris dans le préfixe seront inclus.
> Lorsque vous modifiez l'étendue d'un point d'accès avec l'API, vous remplacez la portée existante.

```
PUT /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
<?xml version="1.0" encoding="UTF-8"?>
<PutAccessPointScopeRequest>
        <Scope>
            <Prefixes>
                <Prefix>Jane/*</Prefix>
            </Prefixes>
            <Permissions>
                <Permission>PutObject</Permission>
                <Permission>GetObject</Permission>
            </Permissions>
            <Scope>
    </PutAccessPointScopeRequest>
```

En utilisant le AWS SDKs

Vous pouvez utiliser l'API AWS CLI AWS SDKs, ou REST pour modifier l'étendue de votre point d'accès. Pour plus d'informations, consultez la liste des produits pris SDKs en charge dans le manuel Amazon Simple Storage Service API Reference.

Supprimez l'étendue de vos points d'accès pour les compartiments d'annuaire

Vous pouvez utiliser l'API REST AWS Management Console AWS Command Line Interface, ou AWS SDKs pour supprimer l'étendue de vos points d'accès pour les buckets de répertoires.

> **Note**
>
> Lorsque vous supprimez l'étendue d'un point d'accès, tous les préfixes et autorisations sont supprimés.

Utilisation de la console S3

Pour supprimer l'étendue du point d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access points for directory buckets.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer.
6. Sélectionnez l'onglet Autorisations.
7. Dans le champ d'application du point d'accès, choisissez Supprimer.
8. Dans le champ pour confirmer cette suppression, tapez « confirmer ». champ, entrez**`confirm`**.
9. Sélectionnez Delete (Supprimer).

En utilisant le AWS CLI

L'`delete-access-point-scope`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour supprimer l'étendue de votre point d'accès.

La commande suivante supprime l'étendue du point d'accès *`my-access-point`* -- *`zoneID`* --xa-s3 for. Compte AWS *`111122223333`*

```
aws s3control delete-access-point-scope --name my-access-point--region-zoneID--xa-s3 --
account-id 111122223333
```

Pour plus d'informations et des exemples, reportez-vous delete-access-point-scopeà la référence des AWS CLI commandes.

Utilisation de l'API REST

La requête suivante supprime l'étendue du point d'accès *my-access-point* -- *zoneID* --xa-s3 for. Compte AWS *111122223333*

```
DELETE /v20180820/accesspoint/my-access-point--zoneID--xa-s3/scope HTTP/1.1
Host: s3express-control.region.amazonaws.com
x-amz-account-id: 111122223333
```

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour supprimer l'étendue de votre point d'accès. Pour plus d'informations, consultez la liste des produits pris SDKs en charge dans le manuel Amazon Simple Storage Service API Reference.

Supprimer votre point d'accès pour les compartiments de répertoire

Cette section explique comment supprimer votre point d'accès à l' AWS Management Console aide de l'API REST, ou AWS SDKs. AWS Command Line Interface

> **Note**
>
> Avant de pouvoir supprimer un bucket de répertoire attaché à un point d'accès, vous devez supprimer le point d'accès.

Utilisation de la console S3

Pour supprimer des points d'accès pour les compartiments de répertoire de votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access points for directory buckets.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez supprimer.
6. Sélectionnez Delete (Supprimer).
7. Pour confirmer la suppression, tapez **`confirm`** et choisissez Supprimer.

En utilisant le AWS CLI

L'`delete-access-point`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour supprimer votre point d'accès.

La commande suivante supprime le point d'accès *`my-access-point`* -- *`zoneID`* --xa-s3 for. Compte AWS *`111122223333`*

```
aws s3control delete-access-point --name my-access-point--zoneID--xa-s3 --account-
id 111122223333
```

Pour plus d'informations et des exemples, consultez delete-access-point dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour supprimer votre point d'accès. Pour plus d'informations, consultez DeleteAccessPoint dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour supprimer vos points d'accès. Pour plus d'informations, consultez la liste des produits pris SDKs en charge dans le manuel Amazon Simple Storage Service API Reference.

Utilisation de balises avec des points d'accès S3 pour les compartiments de répertoire

Une AWS balise est une paire clé-valeur qui contient des métadonnées relatives aux ressources, en l'occurrence les points d'accès Amazon S3 pour les compartiments d'annuaire. Vous pouvez étiqueter les points d'accès lorsque vous les créez ou gérer les balises sur les points d'accès existants. Pour des informations générales sur les balises, consultezMarquage pour la répartition des coûts ou le contrôle d'accès basé sur les attributs (ABAC).

> **Note**
>
> L'utilisation de balises sur les points d'accès pour les buckets de répertoires est gratuite, au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3.

Méthodes courantes d'utilisation des balises avec des points d'accès pour les compartiments de répertoire

Le contrôle d'accès basé sur les attributs (ABAC) vous permet de dimensionner les autorisations d'accès et d'accorder l'accès aux points d'accès pour les compartiments d'annuaire en fonction de leurs balises. Pour plus d'informations sur ABAC dans Amazon S3, consultez Utilisation de balises pour ABAC.

ABAC pour points d'accès S3

Les points d'accès Amazon S3 prennent en charge le contrôle d'accès basé sur les attributs (ABAC) à l'aide de balises. Utilisez des clés de condition basées sur des balises dans vos politiques AWS d'organisation, d'IAM et de points d'accès. Pour les entreprises, l'ABAC d'Amazon S3 prend en charge l'autorisation sur plusieurs AWS comptes.

Dans vos politiques IAM, vous pouvez contrôler l'accès aux points d'accès pour les compartiments d'annuaire en fonction des balises du compartiment à l'aide des clés de condition globales suivantes :

- `aws:ResourceTag/key-name`
  - Utilisez cette clé pour comparer la paire valeur clé d'étiquette que vous spécifiez dans la politique avec la paire valeur clé attachée à la ressource. Par exemple, vous pouvez exiger que l'accès à une ressource soit autorisé uniquement si la clé de balise `Dept` est attachée à la ressource

avec la valeur `Marketing`. Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources.

- `aws:RequestTag/key-name`
  - Utilisez cette clé pour comparer la paire clé-valeur de balise qui a été transmise dans la demande avec la paire de balises spécifiée dans la politique. Par exemple, vous pouvez vérifier que la demande comprend la clé de balise `Dept` et qu'elle a la valeur `Accounting`. Pour plus d'informations, consultez la section Contrôle de l'accès lors AWS des demandes. Vous pouvez utiliser cette clé de condition pour restreindre les paires clé-valeur de balise qui peuvent être transmises pendant les opérations d'`CreateAccessPoint`API `TagResource` et d'API.
- `aws:TagKeys`
  - Utilisez cette clé pour comparer les clés de balise d'une demande avec celles spécifiées dans la politique. Nous vous recommandons, lorsque vous utilisez des politiques pour contrôler l'accès à l'aide de balises, d'utiliser la clé de condition `aws:TagKeys` pour définir quelles clés de balises sont autorisées. Pour des exemples de politiques et pour plus d'informations, consultez la section Contrôle de l'accès en fonction des clés de balise. Vous pouvez créer un point d'accès pour les compartiments de répertoire dotés de balises. Pour autoriser le balisage pendant le fonctionnement de l'`CreateAccessPoint`API, vous devez créer une politique qui inclut à la fois les `s3express:CreateAccessPoint` actions `s3express:TagResource` et. Vous pouvez ensuite utiliser la clé de `aws:TagKeys` condition pour appliquer l'utilisation de balises spécifiques dans la `CreateAccessPoint` demande.
- `s3express:AccessPointTag/tag-key`
  - Utilisez cette clé de condition pour accorder des autorisations à des données spécifiques via des points d'accès utilisant des balises. Lors de l'utilisation `aws:ResourceTag/tag-key` dans le cadre d'une politique IAM, le point d'accès ainsi que le compartiment vers lequel le point d'accès pointe doivent avoir la même balise sont pris en compte lors de l'autorisation. Si vous souhaitez contrôler l'accès à vos données uniquement via la balise de point d'accès, vous pouvez utiliser la clé de `s3express:AccessPointTag/tag-key` condition.

Exemples de politiques ABAC pour les points d'accès aux compartiments d'annuaire

Consultez les exemples de politiques ABAC suivants pour les points d'accès aux compartiments de répertoire.

1.1 - Politique IAM pour créer ou modifier des points d'accès avec des balises spécifiques

Dans cette stratégie IAM, les utilisateurs ou les rôles dotés de cette politique ne peuvent créer des points d'accès que s'ils balisent les points d'accès avec la clé de balise `project` et la valeur de balise `Trinity` dans la demande de création de point d'accès. Ils peuvent également ajouter ou modifier des balises sur les points d'accès existants pour les compartiments de répertoire, à condition que la `TagResource` demande inclut la paire clé-valeur de balise. `project:Trinity`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAccessPointWithTags",
      "Effect": "Allow",
      "Action": [
        "s3express:CreateAccessPoint",
        "s3express:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
            "Trinity"
          ]
        }
      }
    }
  ]
}
```

1.2 - Politique de point d'accès visant à restreindre les opérations sur le bucket à l'aide de balises

Dans cette politique de point d'accès, les principaux IAM (utilisateurs et rôles) peuvent effectuer des opérations à l'aide de l'`CreateSession`action sur le point d'accès uniquement si la valeur de la `project` balise du point d'accès correspond à la valeur de la balise du `project` principal.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
```

```
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3express:CreateSession",
      "Resource": "arn:aws::s3express:region:111122223333:access-point/my-access-
point",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

1.3 - Politique IAM visant à modifier les balises sur les ressources existantes tout en maintenant la gouvernance du balisage

Dans cette politique IAM, les principaux IAM (utilisateurs ou rôles) peuvent modifier les balises d'un point d'accès uniquement si la valeur de la `project` balise du point d'accès correspond à la valeur de la balise du principal. `project` Seules les quatre balises`project`, `environment``owner`, et `cost-center` spécifiées dans les clés de `aws:TagKeys` condition sont autorisées pour ces points d'accès. Cela permet de renforcer la gouvernance des balises, d'empêcher les modifications non autorisées des balises et de garantir la cohérence du schéma de balisage sur l'ensemble de vos points d'accès.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3express:TagResource"
      ],
      "Resource": "arn:aws::s3express:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
```

```
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 - Utilisation de la clé de condition s3express : AccessPointTag

Dans cette politique IAM, l'énoncé de condition autorise l'accès aux données du bucket uniquement si le point d'accès utilisé pour accéder au bucket possède la clé `Environment` et la valeur `Production` de balise.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3express:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "s3express:AccessPointTag/Environment": "Production"
        }
      }
    }
  ]
}
```

Utilisation de balises pour les points d'accès aux compartiments de répertoire

Vous pouvez ajouter ou gérer des balises pour les points d'accès aux compartiments de répertoire à l'aide de la console Amazon S3, de l'interface de ligne de AWS commande (CLI) AWS SDKs, ou à l'aide du S3 APIs : TagResourceUntagResource, et ListTagsForResource. Pour plus d'informations, consultez :

Rubriques

- Création de points d'accès pour les compartiments de répertoire avec des balises
- Ajout d'une balise à un point d'accès pour les compartiments de répertoire
- Afficher les balises d'un point d'accès pour les compartiments de répertoire
- Suppression d'une balise d'un point d'accès pour les compartiments de répertoire

Création de points d'accès pour les compartiments de répertoire avec des balises

Vous pouvez étiqueter les points d'accès Amazon S3 pour les compartiments de répertoire lorsque vous les créez. Pour plus d'informations, consultez Utilisation de balises avec des points d'accès S3 pour les compartiments de répertoire.

Autorisations

Pour créer un point d'accès pour les compartiments de répertoire dotés de balises, vous devez disposer des autorisations suivantes :

- `s3express:CreateAccessPoint`
- `s3express:TagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de créer un point d'accès pour les compartiments de répertoire contenant des balises, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des éléments nécessaires Autorisations pour créer le point d'accès pour les compartiments de répertoire et ajoutez-y une balise.
- Vérifiez votre politique utilisateur IAM pour connaître les conditions de contrôle d'accès basé sur les attributs (ABAC). Vous devrez peut-être étiqueter vos points d'accès pour les compartiments de répertoire uniquement avec des clés et des valeurs de balise spécifiques. Pour de plus amples informations, veuillez consulter Utilisation de balises pour le contrôle d'accès basé sur les attributs (ABAC).

Étapes

Vous pouvez créer un point d'accès pour les compartiments de répertoire avec des balises appliquées à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour créer un point d'accès pour les compartiments de répertoire contenant des balises à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (Directory Buckets).
3. Choisissez Créer un point d'accès pour créer un nouveau point d'accès.
4. Entrez un nom pour le point d'accès. Pour de plus amples informations, veuillez consulter Points d'accès pour les règles de dénomination, restrictions et limitations des compartiments de répertoire.
5. Sur la page Créer un point d'accès, l'option Tags est disponible lors de la création d'un nouveau point d'accès.
6. Choisissez Ajouter une nouvelle balise pour ouvrir l'éditeur de balises et entrez une paire clé-valeur de balise. La clé de balise est obligatoire, mais la valeur est facultative.
7. Pour ajouter une autre étiquette, sélectionnez à nouveau Ajouter une nouvelle étiquette. Vous pouvez saisir jusqu'à 50 paires clé-valeur de balise.
8. Après avoir défini les options pour votre nouveau point d'accès, choisissez Create access point.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment créer un point d'accès avec des balises à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
CreateAccessPointRequest createAccessPointRequest =
 CreateAccessPointRequest.builder()
                .accountId(111122223333)
                .name(my-access-point)
                .bucket(amzn-s3-demo-bucket--zone-id--x-s3)

 .tags(Collections.singletonList(Tag.builder().key("key1").value("value1").build()))
                .build();
 awss3Control.createAccessPoint(createAccessPointRequest);
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la création d'un compartiment de répertoire avec des balises, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- CreateBucket

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant vous montre comment créer un point d'accès pour les compartiments de répertoire avec des balises à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Lorsque vous créez un point d'accès pour les compartiments de répertoire, vous devez fournir les détails de configuration et utiliser la convention de dénomination suivante : *my-access-point*

Requête :

```
aws s3control create-access-point \
--account-id 111122223333 \
--name my-access-point \
--bucket amzn-s3-demo-bucket--zone-id--x-s3 \
--profile personal \
--tags Key=key1,Value=value1 Key=MyKey2,Value=value2 \
--region region
```

Ajout d'une balise à un point d'accès pour les compartiments de répertoire

Vous pouvez ajouter des balises aux points d'accès Amazon S3 pour les compartiments de répertoire et modifier ces balises. Pour plus d'informations, consultez Utilisation de balises avec des points d'accès S3 pour les compartiments de répertoire.

Autorisations

Pour ajouter une balise à un point d'accès pour les compartiments de répertoire, vous devez disposer des autorisations suivantes :

- `s3express:TagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez d'ajouter une balise à un point d'accès pour les compartiments de répertoire, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des conditions requises Autorisations pour ajouter une balise à un point d'accès pour les compartiments de répertoire.
- Si vous avez essayé d'ajouter une clé de balise commençant par le préfixe AWS réservé`aws:`, modifiez la clé de balise et réessayez.

Étapes

Vous pouvez ajouter des balises aux points d'accès pour les compartiments de répertoire à l'aide de la console Amazon S3, de l'interface de ligne de AWS commande (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour ajouter des balises à un point d'accès pour les compartiments de répertoire à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (Directory Buckets).
3. Choisissez le nom du point d'accès.
4. Choisissez l'onglet Propriétés.
5. Accédez à la section Tags et choisissez Ajouter un nouveau tag.
6. Cela ouvre la page Ajouter des balises. Vous pouvez saisir jusqu'à 50 paires clé-valeur de balise.
7. Si vous ajoutez une nouvelle balise portant le même nom de clé qu'une balise existante, la valeur de la nouvelle balise remplace la valeur de la balise existante.
8. Vous pouvez également modifier les valeurs des balises existantes sur cette page.
9. Après avoir ajouté les balises, choisissez Enregistrer les modifications.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment ajouter des balises à un point d'accès pour les compartiments de répertoire à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;
import software.amazon.awssdk.services.s3control.model.TagResourceResponse;

public class TagResourceExample {
    public static void tagResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                .resourceArn("arn:aws::s3:region:111122223333:accesspoint/my-access-
point/*")
                .accountId("111122223333")
                .tags(Tag.builder().key("key1").value("value1").build())
                .build();

        TagResourceResponse response = s3Control.tagResource(tagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour l'ajout de balises à un point d'accès pour les compartiments de répertoire, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- TagResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant montre comment ajouter des balises à un bucket de répertoire à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3express:region:444455556666:bucket/prefix--use1-az4--x-s3 \
--tags "Key=key1,Value=value1"
```

Réponse :

```
{
  "ResponseMetadata": {
      "RequestId": "EXAMPLE123456789",
      "HTTPStatusCode": 200,
      "HTTPHeaders": {
          "date": "Wed, 19 Jun 2025 10:30:00 GMT",
          "content-length": "0"
      },
      "RetryAttempts": 0
  }
}
```

Afficher les balises d'un point d'accès pour les compartiments de répertoire

Vous pouvez afficher ou répertorier les balises appliquées aux points d'accès Amazon S3 pour les compartiments d'annuaire. Pour plus d'informations, consultez Utilisation de balises avec des compartiments de répertoire S3.

Autorisations

Pour afficher les balises appliquées à un point d'accès, vous devez disposer des autorisations suivantes :

- `s3express:ListTagsForResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de répertorier ou d'afficher les balises d'un point d'accès pour les compartiments de répertoire, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des informations requises Autorisations pour afficher ou répertorier les balises du point d'accès pour les compartiments de répertoire.

Étapes

Vous pouvez consulter les balises appliquées aux points d'accès pour les compartiments d'annuaire à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour afficher les balises appliquées à un point d'accès pour les compartiments d'annuaire à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (Directory Buckets).
3. Choisissez le nom du point d'accès.
4. Choisissez l'onglet Propriétés.
5. Accédez à la section Balises pour afficher toutes les balises appliquées au point d'accès pour les compartiments de répertoire.
6. La section Tags affiche les tags définis par l'utilisateur par défaut. Vous pouvez sélectionner l'onglet balises AWS générées pour afficher les balises appliquées à votre point d'accès par les AWS services.

En utilisant le AWS SDKs

Cette section fournit un exemple de la façon d'afficher les balises appliquées à un point d'accès pour les compartiments de répertoire à l'aide du AWS SDKs.

SDK for Java 2.x

Cet exemple montre comment afficher les balises appliquées à un point d'accès pour les compartiments d'annuaire à l'aide du AWS SDK for Java 2.x.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        ListTagsForResourceRequest listTagsForResourceRequest =
 ListTagsForResourceRequest.builder()
                .resourceArn("arn:aws::s3:us-west-2:111122223333:accesspoint/my-
access-point/*")
                .accountId("111122223333")
                .build();
        ListTagsForResourceResponse response =
 s3Control.listTagsForResource(listTagsForResourceRequest);
        System.out.println("Tags on my resource:");
        System.out.println(response.toString());
    }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST d'Amazon S3 pour l'affichage des balises appliquées à un compartiment de répertoire, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- ListTagsforResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant vous montre comment afficher les balises appliquées à un point d'accès pour les compartiments de répertoire. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3express:region:444455556666:bucket/prefix--use1-az4--x-s3 \
```

Réponse : balises présentes :

```
{
  "Tags": [
      {
          "Key": "MyKey1",
          "Value": "MyValue1"
      },
      {
          "Key": "MyKey2",
          "Value": "MyValue2"
      },
      {
          "Key": "MyKey3",
          "Value": "MyValue3"
      }
  ]
}
```

Réponse : aucun tag n'est présent :

```
{
  "Tags": []
}
```

Suppression d'une balise d'un point d'accès pour les compartiments de répertoire

Vous pouvez supprimer des balises des points d'accès pour les compartiments de répertoire. Pour plus d'informations, consultez Utilisation de balises avec des points d'accès S3 pour les compartiments de répertoire.

> **Note**
>
> Si vous supprimez une balise et apprenez par la suite qu'elle était utilisée pour suivre les coûts ou pour contrôler l'accès, vous pouvez la réajouter au point d'accès pour les compartiments de répertoire.

Autorisations

Pour supprimer une balise d'un point d'accès pour les compartiments de répertoire, vous devez disposer des autorisations suivantes :

- `s3express:UntagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de supprimer une balise d'un point d'accès pour les compartiments de répertoire, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des conditions requises Autorisations pour supprimer une balise d'un point d'accès pour les compartiments de répertoire.

Étapes

Vous pouvez supprimer des balises des points d'accès pour les compartiments de répertoire à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour supprimer des balises d'un point d'accès pour les compartiments de répertoire à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (Directory Buckets).
3. Choisissez le nom du point d'accès.
4. Choisissez l'onglet Propriétés.
5. Accédez à la section Tags et cochez la case à côté du tag ou des tags que vous souhaitez supprimer.
6. Sélectionnez Delete (Supprimer).
7. La fenêtre contextuelle Supprimer les balises définies par l'utilisateur apparaît et vous demande de confirmer la suppression de la ou des balises que vous avez sélectionnées.
8. Choisissez Supprimer pour confirmer.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment supprimer des balises d'un bucket de répertoire à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                .resourceArn("arn:aws::s3:region:111122223333:accesspoint/my-access-
point/*")
                .accountId("111122223333")
                .tagKeys("key1")
                .build();

        UntagResourceResponse response =
 s3Control.untagResource(untagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la suppression de balises d'un point d'accès, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- UnTagResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant montre comment supprimer des balises d'un point d'accès à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control untag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3:region:111122223333:accesspoint/my-access-point/* \
--tag-keys "key1" "key2"
```

Réponse :

```
{
  "ResponseMetadata": {
    "RequestId": "EXAMPLE123456789",
    "HTTPStatusCode": 204,
    "HTTPHeaders": {
        "date": "Wed, 19 Jun 2025 10:30:00 GMT",
        "content-length": "0"
    },
    "RetryAttempts": 0
  }
}
```

Journalisation avec AWS CloudTrail des compartiments de répertoire

Amazon S3 est intégré à AWS 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 Amazon S3 sous forme d'événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon S3, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires. Lorsqu'une activité événementielle prise en charge se produit dans Amazon S3, cette activité est enregistrée

dans un CloudTrail événement. Vous pouvez utiliser le journal AWS CloudTrail pour consigner les événements de gestion et les événements de données relatifs aux compartiments de répertoire. Pour plus d'informations, consultez les sections CloudTrail Événements Amazon S3 et Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail événements de gestion pour les compartiments de répertoire

Par défaut, CloudTrail enregistre les actions au niveau du compartiment pour les compartiments de répertoire en tant qu'événements de gestion. Les événements CloudTrail de gestion `eventsource` pour les compartiments de répertoire sont`s3express.amazonaws.com`. Lorsque vous configurez votre AWS compte, les événements CloudTrail de gestion sont activés par défaut. Les opérations d'API de point de terminaison régional suivantes (opérations d'API au niveau du compartiment ou du plan de contrôle, opérations d'API) sont enregistrées. CloudTrail

- `CreateBucket`
- `DeleteBucket`
- `DeleteBucketPolicy`
- `PutBucketPolicy`
- `GetBucketPolicy`
- `ListDirectoryBuckets`
- `ListMultipartUploads`
- `GetBucketEncryption`
- `PutBucketEncryption`
- `DeleteBucketEncryption`

> **Note**
>
> `ListMultipartUploads` est une opération d'API de point de terminaison zonal. Toutefois, cette opération d'API est enregistrée en CloudTrail tant qu'événement de gestion. Pour plus d'informations, consultez `ListMultipartUploads` dans la Référence d'API Amazon Simple Storage Service.

Pour plus d'informations sur les événements CloudTrail de gestion, consultez la section Journalisation des événements de gestion dans le Guide de AWS CloudTrail l'utilisateur.

CloudTrail événements de données pour les compartiments de répertoire

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 dont le volume est élevé. Par défaut, les CloudTrail sentiers n'enregistrent pas les événements de données, mais vous pouvez configurer les sentiers pour qu'ils enregistrent les événements de données pour les objets stockés dans des compartiments à usage général et des compartiments de répertoire. Pour plus d'informations, consultez Activation de la journalisation des objets d'un compartiment à l'aide de la console.

Lorsque vous enregistrez des événements de données pour un trail in CloudTrail, vous pouvez choisir d'utiliser des sélecteurs d'événements avancés ou des sélecteurs d'événements de base. Pour journaliser des événements de données pour des objets stockés dans des compartiments de répertoires, vous devez utiliser des sélecteurs d'événements avancés. Lors de la configuration des sélecteurs de ressources avancés, vous devez choisir ou spécifier le type de ressource qui est `AWS::S3Express::Object`.

Les opérations d'API de point de terminaison zonales suivantes (au niveau de l'objet, ou du plan de données, opérations d'API) sont enregistrées. CloudTrail

- `AbortMultipartUpload`
- `CompleteMultipartUpload`
- `CreateSession`
- `CopyObject`
- `CreateMultipartUpload`
- `DeleteObject`
- `DeleteObjects`
- `GetObject`
- `GetObjectAttributes`
- `HeadBucket`
- `HeadObject`
- `ListObjectsV2`
- `ListParts`
- `PutObject`

- RenameObject
- UploadPart
- UploadPartCopy

Pour plus d'informations sur les événements CloudTrail liés aux données, consultez la section Enregistrement des événements liés aux données dans le Guide de AWS CloudTrail l'utilisateur.

Pour plus d'informations sur les CloudTrail événements relatifs aux compartiments de répertoire, consultez les rubriques suivantes :

Rubriques

- CloudTrail exemples de fichiers journaux pour les compartiments de répertoires

CloudTrail exemples de fichiers journaux pour les compartiments de répertoires

Un fichier CloudTrail journal contient des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. Cette rubrique contient des exemples d'événements de CloudTrail données et d'événements de gestion pour les compartiments d'annuaire.

Rubriques

- CloudTrail exemples de fichiers journaux d'événements de données pour les compartiments de répertoires

CloudTrail exemples de fichiers journaux d'événements de données pour les compartiments de répertoires

L'exemple suivant montre un exemple de fichier CloudTrail journal qui illustre CreateSession.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
      "type": "AssumedRole",
      "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
      "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
          "sessionContext": {
            "sessionIssuer": {
              "type": "Role",
              "principalId": "AROAIDPPEZS35WEXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/RoleToBeAssumed",
              "accountId": "111122223333",
              "userName":"RoleToBeAssumed
            },

            "attributes": {
              "creationDate": "2024-07-02T00:21:16Z",
            "mfaAuthenticated": "false"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:11Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "CreateSession",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.20.160-SNAPSHOT
 Linux/5.10.216-225.855.amzn2.x86_64 OpenJDK_64-Bit_Server_VM/11.0.23+9-LTS
 Java/11.0.23 vendor/Amazon.com_Inc. md/internal exec-env/AWS_Lambda_java11 io/sync
 http/Apache cfg/retry-mode/standard",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3".
            "host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
            "x-amz-create-session-mode": "ReadWrite"
        },
        "responseElements": {
            "credentials": {
                "accessKeyId": "AKIAI44QH8DHBEXAMPLE"
                "expiration": ""Mar 20, 2024, 11:16:09 PM",
                "sessionToken": "<session token string>"
           },
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "TLS_AES_128_GCM_SHA256",
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhNJYmhg",
            "bytesTransferredOut": 1815,
```

```
            "availabilityZone": "usw2-az1"
          },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
          "resources": [
            {
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
            },
            {
              "accountId": "111122223333"
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
             }
           ],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.3",
             "cipherSuite": "TLS_AES_128_GCM_SHA256",
             "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
            }
          }
```

Pour utiliser les opérations d'API de point de terminaison zonal (opérations de niveau objet ou plan de données), optez pour l'opération d'API `CreateSession` pour créer et gérer des sessions optimisées afin d'autoriser les demandes de données à faible latence. Vous pouvez également utiliser `CreateSession` pour réduire le volume de journalisation. Pour identifier les opérations d'API zonales effectuées au cours d'une session, vous pouvez faire correspondre l'`accessKeyId` sous `responseElements` dans votre fichier journal `CreateSession` à l'`accessKeyId` dans le fichier journal des autres opérations d'API zonales. Pour plus d'informations, consultez Autorisation `CreateSession`.

L'exemple suivant montre un exemple de fichier CloudTrail journal qui illustre l'opération d'`GetObject`API authentifiée par`CreateSession`.

```
    {
        "eventVersion": "1.09",
        "userIdentity": {
          "type": "AssumedRole",
          "principalId": "AROAIDPPEZS35WEXAMPLE:AssumedRoleSessionName",
          "arn": "arn:aws:sts::111122223333assumed-role/RoleToBeAssumed/MySessionName",
          "accountId": "111122223333",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "sessionContext": {
            "attributes": {
              "creationDate": "2024-07-02T00:21:49Z"
            }
          }
        },
        "eventTime": "2024-07-02T00:22:01Z",
        "eventSource": "s3express.amazonaws.com",
        "eventName": "GetObject",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "72.21.198.68",
        "userAgent": "aws-sdk-java/2.25.66 Linux/5.10.216-225.855.amzn2.x86_64
 OpenJDK_64-Bit_Server_VM/17.0.11+9-LTS Java/17.0.11 vendor/Amazon.com_Inc. md/internal
 exec-env/AWS_Lambda_java17 io/sync http/Apache cfg/retry-mode/legacy",
        "requestParameters": {
          "bucketName": "bucket-base-name--usw2-az1--x-s3",
          "x-amz-checksum-mode": "ENABLED",
          "Host": "bucket-base-name--usw2-az1--x-s3.s3express-usw2-az1.us-
west-2.amazonaws.com",
          "key": "test-get-obj-with-checksum"
        },
        "responseElements": null,
        "additionalEventData": {
          "SignatureVersion": "Sigv4",
          "CipherSuite": "TLS_AES_128_GCM_SHA256",
          "bytesTransferredIn": 0,
          "AuthenticationMethod": "AuthHeader",
          "x-amz-id-2": "oOy6w8K7LFsyFN",
          "bytesTransferredOut": 9,
          "availabilityZone": "usw2-az1",
          "sessionModeApplied": "ReadWrite"
         },
          "requestID": "28d2faaf-3319-4649-998d-EXAMPLE72818",
          "eventID": "694d604a-d190-4470-8dd1-EXAMPLEe20c1",
          "readOnly": true,
```

```
          "resources": [
            {
              "type": "AWS::S3Express::Object",
              "ARNPrefix": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--
usw2-az1--x-s3"
            },
            {
              "accountId": "111122223333",
              "type": "AWS::S3Express::DirectoryBucket",
              "ARN": "arn:aws:s3express:us-west-2:111122223333:bucket-base-name--usw2-
az1--x-s3"
             }
           ],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "111122223333",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.3",
             "cipherSuite": "TLS_AES_128_GCM_SHA256",
             "clientProvidedHostHeader": "bucket-base-name--usw2-az1--x-s3.s3express-
usw2-az1.us-west-2.amazonaws.com"
            }
          }
```

Dans l'exemple de fichier `GetObject` journal ci-dessus, le `accessKeyId` (AKIAI44QH8DHBEXAMPLE) correspond `responseElements` à l'`accessKeyId`exemple de fichier CreateSession journal ci-dessous. La correspondance de l'`accessKeyId` indique la session au cours de laquelle l'opération `GetObject` a été effectuée.

L'exemple suivant montre une entrée de CloudTrail journal qui illustre une `DeleteObjects` action sur un compartiment de répertoire, invoqué par S3 Lifecycle. Pour de plus amples informations, veuillez consulter Working with S3 Lifecycle for directory buckets.

```
eventVersion:"1.09",
  userIdentity:{

    type:"AWSService",
    invokedBy:"lifecycle.s3.amazonaws.com"
  },
  eventTime:"2024-09-11T00:55:54Z",
  eventSource:"s3express.amazonaws.com",
```

```
  eventName:"DeleteObjects",
  awsRegion:"us-east-2",
  sourceIPAddress:"lifecycle.s3.amazonaws.com",
  userAgent:"gamma.lifecycle.s3.amazonaws.com",
  requestParameters:{

    bucketName:"amzn-s3-demo-bucket--use2-az2--x-s3",
    'x-amz-expected-bucket-owner':"637423581905",
    Host:"amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-az2.express.s3.aws.dev",
    delete:"",
    'x-amz-sdk-checksum-algorithm':"CRC32C"
  },
  responseElements:null,
  additionalEventData:{

    SignatureVersion:"Sigv4",
    CipherSuite:"TLS_AES_128_GCM_SHA256",
    bytesTransferredIn:41903,
    AuthenticationMethod:"AuthHeader",
    'x-amz-id-2':"9H5YWZY0",
    bytesTransferredOut:35316,
    availabilityZone:"use2-az2",
    sessionModeApplied:"ReadWrite"
  },
  requestID:"011eeadd04000191",
  eventID:"d3d8b116-219d-4ee6-a072-5f9950733c74",
  readOnly:false,
  resources:[

    {

      type:"AWS::S3Express::Object",
      ARNPrefix:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--
use2-az2--x-s3/"
    },
    {

      accountId:"637423581905",
      type:"AWS::S3Express::DirectoryBucket",
      ARN:"arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-bucket--use2-
az2--x-s3"
    }
  ],
  eventType:"AwsApiCall",
```

```
  managementEvent:false,
  recipientAccountId:"637423581905",
  sharedEventID:"59f877ac-1dd9-415d-b315-9bb8133289ce",
  eventCategory:"Data"
}
```

L'exemple suivant montre une entrée de CloudTrail journal qui illustre une `Access Denied` demande concernant une `CreateSession` action invoquée par S3 Lifecycle. Pour de plus amples informations, veuillez consulter CreateSession.

```
{
    "eventVersion": "1.09",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "gamma.lifecycle.s3.amazonaws.com"
    },
    "eventTime": "2024-09-11T18:13:08Z",
    "eventSource": "s3express.amazonaws.com",
    "eventName": "CreateSession",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "gamma.lifecycle.s3.amazonaws.com",
    "userAgent": "gamma.lifecycle.s3.amazonaws.com",
    "errorCode": "AccessDenied",
    "errorMessage": "Access Denied",
    "requestParameters": {
        "bucketName": "amzn-s3-demo-bucket--use2-az2--x-s3",
        "Host": "amzn-s3-demo-bucket--use2-az2--x-s3.gamma.use2-
az2.express.s3.aws.dev",
        "x-amz-create-session-mode": "ReadWrite",
        "x-amz-server-side-encryption": "AES256"
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "Sigv4",
        "CipherSuite": "TLS_AES_128_GCM_SHA256",
        "bytesTransferredIn": 0,
        "AuthenticationMethod": "AuthHeader",
        "x-amz-id-2": "zuDDC1VNbC4LoNwUIc5",
        "bytesTransferredOut": 210,
        "availabilityZone": "use2-az2"
    },
    "requestID": "010932f174000191e24a0",
    "eventID": "dce7cc46-4cd3-46c0-9a47-d1b8b70e301c",
```

```
    "readOnly": true,
    "resources": [{
            "type": "AWS::S3Express::Object",
            "ARNPrefix": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3/"
        },
        {
            "accountId": "637423581905",
            "type": "AWS::S3Express::DirectoryBucket",
            "ARN": "arn:aws:s3express:us-east-2:637423581905:bucket/amzn-s3-demo-
bucket--use2-az2--x-s3"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "637423581905",
    "sharedEventID": "da96b5bd-6066-4a8d-ad8d-f7f427ca7d58",
    "eventCategory": "Data"
}
```

Optimisation des performances des compartiments de répertoires

Pour optimiser les performances lorsque vous utilisez des compartiments de répertoires, nous recommandons les consignes suivantes.

Pour plus d'informations sur les meilleures pratiques relatives à S3 Express One Zone, consultezMeilleures pratiques pour optimiser les performances de S3 Express One Zone.

Utilisation de l'authentification basée sur les sessions

Les compartiments de répertoires prennent en charge un nouveau mécanisme d'autorisation basé sur les sessions pour authentifier et autoriser les demandes adressées à un compartiment de répertoires. Avec l'authentification basée sur les sessions, ils utilisent AWS SDKs automatiquement l'opération `CreateSession` API pour créer un jeton de session temporaire qui peut être utilisé pour autoriser à faible latence les demandes de données adressées à un bucket d'annuaire.

Ils AWS SDKs utilisent l'opération `CreateSession` API pour demander des informations d'identification temporaires, puis créent et actualisent automatiquement des jetons pour vous en votre nom toutes les 5 minutes. Pour tirer parti des avantages des buckets d'annuaire en termes de

performances, nous vous recommandons d'utiliser le AWS SDKs pour lancer et gérer la demande `CreateSession` d'API. Pour plus d'informations sur ce modèle basé sur les sessions, consultez Autorisation des opérations d'API de point de terminaison zonal avec `CreateSession`.

Bonnes pratiques supplémentaires en matière de somme de contrôle S3

Les compartiments de répertoires vous offrent la possibilité de sélectionner l'algorithme de somme de contrôle utilisé pour valider vos données pendant le chargement ou le téléchargement. Vous pouvez sélectionner l'un des algorithmes de hachage sécurisé (SHA) ou de contrôle de redondance cyclique (CRC) suivants : CRC32 C CRC32, SHA-1 et SHA-256. MD5les checksums basés sur la base de données ne sont pas pris en charge avec la classe de stockage S3 Express One Zone.

CRC32 est la somme de contrôle par défaut utilisée par le AWS SDKs lors de la transmission de données vers ou depuis des compartiments de répertoire. Nous vous recommandons d'utiliser CRC32 et CRC32 C pour optimiser les performances avec les buckets de répertoires.

Utiliser la dernière version des bibliothèques d'exécution AWS SDKs et les bibliothèques d'exécution communes

Plusieurs d'entre eux fournissent AWS SDKs également les bibliothèques AWS Common Runtime (CRT) pour accélérer encore les performances des clients S3. Ceux-ci SDKs incluent le AWS SDK for Java 2.x, le AWS SDK pour C++, et le AWS SDK pour Python (Boto3). Le client S3 basé sur CRT transfère des objets vers et depuis des compartiments de répertoires avec des performances et une fiabilité améliorées en utilisant automatiquement l'opération d'API de chargement partitionné et les extractions de plages d'octets pour automatiser la mise à l'échelle horizontale des connexions.

Pour obtenir les meilleures performances avec les compartiments de répertoires, nous vous recommandons d'utiliser la dernière version AWS SDKs qui inclut les bibliothèques CRT ou d'utiliser le AWS Command Line Interface ()AWS CLI.

Développement avec des compartiments de répertoires

Une fois que vous avez créé votre compartiment de répertoires, vous pouvez immédiatement commencer des opérations de lecture et d'écriture à très faible latence. Vous pouvez communiquer avec votre compartiment de répertoires à l'aide d'une connexion de point de terminaison via un cloud privé virtuel (VPC), ou vous pouvez utiliser les opérations d'API zonales et régionales pour gérer vos objets et compartiments de répertoires. Vous pouvez utiliser des compartiments de répertoires à

l'aide de la console Amazon S3 AWS SDKs, de l'interface de ligne de AWS commande (AWS CLI) et d'Amazon S3 REST APIs.

Rubriques

- Points de terminaison d'API régionaux et zonaux des compartiments de répertoires
- Utilisation de compartiments de répertoires à l'aide de la console S3 AWS CLI, et AWS SDKs
- Opérations d'API des compartiments de répertoires

Points de terminaison d'API régionaux et zonaux des compartiments de répertoires

Pour accéder aux points de terminaison régionaux et zonaux des compartiments de répertoires depuis votre cloud privé virtuel (VPC), vous pouvez utiliser des points de terminaison de VPC de passerelle. Après avoir créé un point de terminaison de passerelle, vous pouvez l'ajouter comme cible dans votre table de routage pour le trafic destiné à compartiment depuis votre VPC. Il n'y a pas de frais supplémentaires pour l'utilisation de points de terminaison de passerelle. Pour plus d'informations sur la manière de configurer des points de terminaison de VPC de passerelle, consultez Mise en réseau des compartiments de répertoires.

Les opérations d'API de niveau compartiment (plan de contrôle) sont disponibles via les points de terminaison régionaux et sont appelées opérations d'API de point de terminaison régional. `CreateBucket` et `DeleteBucket` sont des exemples d'opérations d'API de point de terminaison régional.

Vous utilisez des opérations d'API de point de terminaison zonal (niveau objet ou plan de données) pour charger et gérer vos objets. Les opérations d'API de point de terminaison zonal sont disponibles via un point de terminaison zonal. `PutObject` et `CopyObject` sont des exemples d'opérations d'API zonales.

Pour plus d'informations sur les points de terminaison régionaux et zonaux pour les compartiments de répertoires dans les zones de disponibilité, consultez Points de terminaison régionaux et zonaux pour les compartiments de répertoires d'une zone de disponibilité.

Pour plus d'informations sur les points de terminaison régionaux et zonaux pour les compartiments de répertoires dans les zones locales, consultez Concepts relatifs aux compartiments de répertoires dans les zones locales.

Utilisation de compartiments de répertoires à l'aide de la console S3 AWS CLI, et AWS SDKs

Vous pouvez utiliser la classe de stockage et les compartiments de répertoire S3 Express One Zone à l'aide de la AWS SDKs console Amazon S3 AWS Command Line Interface (AWS CLI) et de l'API REST Amazon S3.

Console S3

Pour bien démarrer avec la console S3, effectuez les étapes suivantes :

- Création de compartiments de répertoires dans une zone de disponibilité
- Vidage d'un compartiment de répertoires
- Suppression d'un compartiment de répertoires

Pour un didacticiel complet, consultez Didacticiel : bien démarrer avec S3 Express One Zone.

AWS SDKs

S3 Express One Zone prend en charge les éléments suivants AWS SDKs :

- AWS SDK pour C++
- AWS SDK pour Go v2
- AWS SDK for Java 2.x
- AWS SDK pour JavaScript v3
- AWS SDK pour .NET
- AWS SDK pour PHP
- AWS SDK pour Python (Boto3)
- AWS SDK pour Ruby
- AWS SDK pour Kotlin
- Kit AWS SDK pour Rust

Lorsque vous travaillez avec S3 Express One Zone, nous vous recommandons d'utiliser la dernière version du AWS SDKs. La zone prise en AWS SDKs charge par S3 Express One gère

l'établissement, le rafraîchissement et la résiliation des sessions en votre nom. Cela signifie que vous pouvez immédiatement commencer à utiliser les opérations d'API après avoir téléchargé, installé AWS SDKs et configuré les autorisations IAM nécessaires. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM.

Pour plus d'informations sur les AWS SDKs, notamment sur la manière de les télécharger et de les installer, consultez la section Outils sur lesquels vous pouvez vous appuyer AWS.

Pour des exemples de AWS SDK, consultez ce qui suit :

- Création de compartiments de répertoires dans une zone de disponibilité
- Vidage d'un compartiment de répertoires
- Suppression d'un compartiment de répertoires

AWS Command Line Interface (AWS CLI)

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour créer des compartiments de répertoires et utiliser les opérations d'API de point de terminaison régionales et zonales prises en charge pour S3 Express One Zone.

Pour commencer à utiliser le AWS CLI, voir Commencer avec le AWS CLI dans le manuel de référence des AWS CLI commandes.

> **Note**
>
> Pour utiliser des compartiments de répertoire avec les `aws s3` commandes de haut niveau, installez AWS CLI la dernière version. Pour plus d'informations sur l'installation et la configuration du AWS CLI, voir Installer ou mettre à jour la dernière version du AWS CLI dans le manuel de référence des AWS CLI commandes.

Pour AWS CLI des exemples, consultez ce qui suit :

- Création de compartiments de répertoires dans une zone de disponibilité
- Vidage d'un compartiment de répertoires
- Suppression d'un compartiment de répertoires

Opérations d'API des compartiments de répertoires

Pour gérer les compartiments de répertoires, vous pouvez utiliser les opérations d'API de point de terminaison régional (au niveau du compartiment, ou plan de contrôle). Pour gérer les objets dans vos compartiments de répertoires, vous pouvez utiliser les opérations d'API de point de terminaison zonal (au niveau de l'objet, ou plan de données). Pour plus d'informations, consultez Mise en réseau des compartiments de répertoires et Points de terminaison et points de terminaison de VPC de passerelle.

Opérations d'API de point de terminaison régional

Les opérations d'API de point de terminaison régionales suivantes sont prises en charge pour les buckets d'annuaires :

- CreateAccessPoint
- CreateBucket
- DeleteAccessPoint
- DeleteAccessPointPolicy
- DeleteAccessPointScope
- DeleteBucket
- DeleteBucketLifecycle
- DeleteBucketPolicy
- GetAccessPoint
- GetAccessPointPolicy
- GetAccessPointScope
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- ListAccessPointsForDirectoryBuckets
- ListDirectoryBuckets
- ListTagsForResource
- PutAccessPointPolicy
- PutAccessPointScope
- PutBucketLifecycleConfiguration

- PutBucketPolicy
- DeleteBucketEncryption
- GetBucketEncryption
- PutBucketEncryption
- TagResource
- UntagResource

Opérations d'API de point de terminaison zonal

Les opérations d'API de point de terminaison zonales suivantes sont prises en charge pour les buckets de répertoires :

- CreateSession
- CopyObject
- DeleteObject
- DeleteObjects
- GetObject
- GetObjectAttributes
- HeadBucket
- HeadObject
- ListObjectsV2
- PutObject
- RenameObject
- AbortMultipartUpload
- CompleteMultiPartUpload
- CreateMultipartUpload
- ListMultipartUploads
- ListParts
- UploadPart
- UploadPartCopy

Utilisation de balises avec des compartiments de répertoire S3

Une AWS balise est une paire clé-valeur qui contient des métadonnées relatives aux ressources, en l'occurrence les compartiments d'annuaire Amazon S3. Vous pouvez étiqueter les compartiments de répertoire S3 lorsque vous les créez ou gérer les balises sur les compartiments de répertoire existants. Pour des informations générales sur les balises, consultezMarquage pour la répartition des coûts ou le contrôle d'accès basé sur les attributs (ABAC).

> **Note**
>
> L'utilisation de balises sur des compartiments de répertoire est gratuite, au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3.

Méthodes courantes d'utilisation des balises avec les compartiments de répertoire

Utilisez des balises sur les compartiments de votre répertoire S3 pour :

1. Répartition des coûts — Suivez les coûts de stockage par compartiment AWS Billing and Cost Management. Pour plus d'informations, consultez la section Utilisation de balises pour ABAC.
2. Contrôle d'accès basé sur les attributs (ABAC) : adaptez les autorisations d'accès et accordez l'accès aux compartiments de répertoire S3 en fonction de leurs balises. Pour plus d'informations, consultez la section Utilisation de balises pour ABAC.

> **Note**
>
> Vous pouvez utiliser les mêmes balises pour la répartition des coûts et le contrôle d'accès.

ABAC pour compartiments de répertoire S3

Les compartiments d'annuaire Amazon S3 prennent en charge le contrôle d'accès basé sur les attributs (ABAC) à l'aide de balises. Utilisez des clés de condition basées sur des balises dans vos AWS politiques d'organisation, d'IAM et de bucket d'annuaire S3. Pour les entreprises, l'ABAC d'Amazon S3 prend en charge l'autorisation sur plusieurs AWS comptes.

Dans vos politiques IAM, vous pouvez contrôler l'accès aux compartiments du répertoire S3 en fonction des balises du compartiment à l'aide des clés de condition globales suivantes :

- `aws:ResourceTag/key-name`
  - Utilisez cette clé pour comparer la paire valeur clé d'étiquette que vous spécifiez dans la politique avec la paire valeur clé attachée à la ressource. Par exemple, vous pouvez exiger que l'accès à une ressource soit autorisé uniquement si la clé de balise `Dept` est attachée à la ressource avec la valeur `Marketing`. Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources.
- `aws:RequestTag/key-name`
  - Utilisez cette clé pour comparer la paire clé-valeur de balise qui a été transmise dans la demande avec la paire de balises spécifiée dans la politique. Par exemple, vous pouvez vérifier que la demande comprend la clé de balise `Dept` et qu'elle a la valeur `Accounting`. Pour plus d'informations, consultez la section Contrôle de l'accès lors AWS des demandes. Vous pouvez utiliser cette clé de condition pour restreindre les paires clé-valeur de balise qui peuvent être transmises pendant les opérations d'`CreateBucket`API `TagResource` et d'API.
- `aws:TagKeys`
  - Utilisez cette clé pour comparer les clés de balise d'une demande avec celles spécifiées dans la politique. Nous vous recommandons, lorsque vous utilisez des politiques pour contrôler l'accès à l'aide de balises, d'utiliser la clé de condition `aws:TagKeys` pour définir quelles clés de balises sont autorisées. Pour des exemples de politiques et pour plus d'informations, consultez la section Contrôle de l'accès en fonction des clés de balise. Vous pouvez créer un compartiment de répertoire S3 avec des balises. Pour autoriser le balisage pendant le fonctionnement de l'`CreateBucket`API, vous devez créer une politique qui inclut à la fois les `s3express:CreateBucket` actions `s3express:TagResource` et. Vous pouvez ensuite utiliser la clé de `aws:TagKeys` condition pour appliquer l'utilisation de balises spécifiques dans la `CreateBucket` demande.
- `s3express:BucketTag/tag-key`
  - Utilisez cette clé de condition pour accorder des autorisations à des données spécifiques dans des compartiments de répertoire à l'aide de balises. Lorsque vous accédez à un compartiment de répertoire à l'aide d'un point d'accès, cette clé de condition fait référence aux balises du compartiment de répertoire à la fois lors de l'autorisation accordée au point d'accès et au compartiment de répertoire, tandis qu'elle ne `aws:ResourceTag/tag-key` référencera les balises que de la ressource pour laquelle elle est autorisée.

Exemples de politiques ABAC pour les compartiments de répertoires

Consultez les exemples de politiques ABAC suivants pour les compartiments d'annuaire Amazon S3.

1.1 - Politique IAM pour créer ou modifier des buckets avec des balises spécifiques

Dans cette politique IAM, les utilisateurs ou les rôles dotés de cette politique ne peuvent créer des compartiments d'annuaire S3 que s'ils balisent le compartiment avec la clé `project` et la valeur de balise `Trinity` dans la demande de création de compartiment. Ils peuvent également ajouter ou modifier des balises sur des compartiments de répertoire S3 existants tant que la `TagResource` demande inclut la paire clé-valeur de balise. `project:Trinity` Cette politique n'accorde aucune autorisation de lecture, d'écriture ou de suppression sur les compartiments ou leurs objets.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateBucketWithTags",
      "Effect": "Allow",
      "Action": [
        "s3express:CreateBucket",
        "s3express:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
            "Trinity"
          ]
        }
      }
    }
  ]
}
```

1.2 - Politique de compartiment visant à restreindre les opérations sur le compartiment à l'aide de balises

Dans cette politique de compartiment, les principaux IAM (utilisateurs et rôles) peuvent effectuer des opérations à l'aide de l'`CreateSession`action sur le compartiment uniquement si la valeur de la `project` balise du compartiment correspond à la valeur de la balise du `project` principal.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3express:CreateSession",
      "Resource": "arn:aws::s3express:us-west-2:111122223333:bucket/amzn-s3-demo-
bucket--usw2-az1--x-s3",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

1.3 - Politique IAM visant à modifier les balises sur les ressources existantes tout en maintenant la gouvernance du balisage

Dans cette politique IAM, les principaux IAM (utilisateurs ou rôles) peuvent modifier les balises d'un bucket uniquement si la valeur de la `project` balise du bucket correspond à la valeur de la balise du principal. `project` Seules les quatre balises`project`, `environment`, `owner`, et `cost-center` spécifiées dans les clés de `aws:TagKeys` condition sont autorisées pour ces compartiments de répertoire. Cela permet de renforcer la gouvernance des balises, d'empêcher les modifications non autorisées des balises et de garantir la cohérence du schéma de balisage dans tous vos compartiments.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3express:TagResource"
      ],
      "Resource": "arn:aws::s3express:us-west-2:111122223333:bucket/*",
```

```
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 - Utilisation de la clé de condition s3express : BucketTag

Dans cette politique IAM, l'énoncé de condition autorise l'accès aux données du bucket uniquement si le bucket possède la clé de balise `Environment` et la valeur `Production` de balise.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3express:us-west-2:111122223333:accesspoint/*",
      "Condition": {
        "StringEquals": {
          "s3express:BucketTag/Environment": "Production"
        }
      }
    }
  ]
}
```

Gestion des balises pour les compartiments de répertoires

Vous pouvez ajouter ou gérer des balises pour les compartiments de répertoire S3 à l'aide de la console Amazon S3, de l'interface de ligne de AWS commande (CLI) ou du S3 APIs :

TagResourceUntagResource, et ListTagsForResource. AWS SDKs Pour plus d'informations, consultez :

Rubriques

- Création de compartiments de répertoire avec des balises
- Ajouter une balise à un bucket de répertoire
- Affichage des balises de bucket du répertoire
- Supprimer un tag d'un bucket de répertoire

Création de compartiments de répertoire avec des balises

Vous pouvez baliser les compartiments de répertoire Amazon S3 lorsque vous les créez. L'utilisation de balises sur des compartiments de répertoire est gratuite, au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3. Pour plus d'informations sur le balisage des compartiments de répertoire, consultez. Utilisation de balises avec des compartiments de répertoire S3

Autorisations

Pour créer un bucket de répertoire avec des balises, vous devez disposer des autorisations suivantes :

- `s3express:CreateBucket`
- `s3express:TagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de créer un bucket de répertoire avec des balises, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des informations nécessaires Autorisations pour créer le bucket de répertoire et y ajouter une balise.
- Vérifiez votre politique utilisateur IAM pour connaître les conditions de contrôle d'accès basé sur les attributs (ABAC). Il se peut que vous deviez étiqueter vos compartiments de répertoire uniquement avec des clés et des valeurs de balise spécifiques. Pour de plus amples informations, veuillez consulter Utilisation de balises pour le contrôle d'accès basé sur les attributs (ABAC).

Étapes

Vous pouvez créer un compartiment de répertoire avec des balises appliquées à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour créer un compartiment de répertoire avec des balises à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez des compartiments de répertoire.
3. Choisissez Create Bucket pour créer un nouveau bucket de répertoire.
4. Vous pouvez créer deux types de compartiments de répertoire :

   Créez un bucket d'annuaire dans une zone de disponibilité pour une charge de travail à hautes performances. Pour de plus amples informations, veuillez consulter Charges de travail hautes performances.

   Créez un compartiment de répertoire dans une zone locale pour une charge de travail de résidence de données. Pour de plus amples informations, veuillez consulter Charges de travail liées à la résidence des données.
5. Pour les deux types de compartiments de répertoire, sur la page Créer un compartiment, l'option Tags est une option lors de la création d'un nouveau compartiment de répertoire.
6. Entrez un nom pour le compartiment. Pour de plus amples informations, veuillez consulter Règles de dénomination des compartiments de répertoires.
7. Choisissez Ajouter une nouvelle balise pour ouvrir l'éditeur de balises et entrez une paire clé-valeur de balise. La clé de balise est obligatoire, mais la valeur est facultative.
8. Pour ajouter une autre étiquette, sélectionnez à nouveau Ajouter une nouvelle étiquette. Vous pouvez saisir jusqu'à 50 paires clé-valeur de balise.
9. Après avoir défini les options de votre nouveau compartiment de répertoire, choisissez Create bucket.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment créer un bucket de répertoire avec des balises à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketInfo;
import software.amazon.awssdk.services.s3.model.BucketType;
import software.amazon.awssdk.services.s3.model.CreateBucketConfiguration;
import software.amazon.awssdk.services.s3.model.CreateBucketRequest;
import software.amazon.awssdk.services.s3.model.CreateBucketResponse;
import software.amazon.awssdk.services.s3.model.DataRedundancy;
import software.amazon.awssdk.services.s3.model.LocationInfo;
import software.amazon.awssdk.services.s3.model.LocationType;
import software.amazon.awssdk.services.s3.model.Tag;

public class CreateBucketWithTagsExample {
    public static void createBucketWithTagsExample() {
        S3Client s3 = S3Client.builder().region(Region.US_WEST_2).build();

        CreateBucketConfiguration bucketConfiguration =
 CreateBucketConfiguration.builder()
                .location(LocationInfo.builder()
                        .type(LocationType.AVAILABILITY_ZONE)
                        .name("usw2-az1").build())
                .bucket(BucketInfo.builder()
                        .type(BucketType.DIRECTORY)
                        .dataRedundancy(DataRedundancy.SINGLE_AVAILABILITY_ZONE)
                        .build())
                .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
                .build();

        CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
                .bucket("amzn-s3-demo-bucket--usw2-az1--x-s3--usw2-az1--x-s3")
                .createBucketConfiguration(bucketConfiguration)
                .build();

        CreateBucketResponse response = s3.createBucket(createBucketRequest);
        System.out.println("Status code (should be 200):");
```

```
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la création d'un compartiment de répertoire avec des balises, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- CreateBucket

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant vous montre comment créer un compartiment de répertoire avec des balises à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Lorsque vous créez un compartiment de répertoires, vous devez fournir les détails de configuration et utiliser la convention de dénomination suivante : *bucket-base-name*--*zone-id*--x-s3

Requête :

```
aws s3api create-bucket \
--bucket bucket-base-name--zone-id--x-s3 \
--create-bucket-configuration "Location={Type=AvailabilityZone,Name=zone-
id},Bucket={DataRedundancy=SingleAvailabilityZone,Type=Directory},Tags=[{Key=mykey1,Value=myval
 {Key=mykey2,Value=myvalue2}]"
```

Réponse :

```
{
  "Location": "http://bucket--use1-az4--x-s3.s3express-use1-az4.us-
east-1.amazonaws.com/"
}
```

Ajouter une balise à un bucket de répertoire

Vous pouvez ajouter des balises aux compartiments de répertoire Amazon S3 et modifier ces balises. L'utilisation de balises sur des compartiments de répertoire est gratuite, au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3. Pour plus d'informations sur le balisage des compartiments de répertoire, consultez. Utilisation de balises avec des compartiments de répertoire S3

Autorisations

Pour ajouter une balise à un bucket de répertoire, vous devez disposer des autorisations suivantes :

- `s3express:TagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez d'ajouter une balise à un bucket de répertoire, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des conditions requises Autorisations pour ajouter une balise à un bucket de répertoire.
- Si vous avez essayé d'ajouter une clé de balise commençant par le préfixe AWS réservé`aws:`, modifiez la clé de balise et réessayez.

Étapes

Vous pouvez ajouter des balises aux compartiments de répertoire à l'aide de la console Amazon S3, de l'interface de ligne de AWS commande (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour ajouter des balises à un compartiment de répertoire à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez des compartiments de répertoire.
3. Choisissez le nom du compartiment.
4. Choisissez l'onglet Propriétés.

5. Accédez à la section Tags et choisissez Ajouter un nouveau tag.
6. Cela ouvre la page Ajouter des balises. Vous pouvez saisir jusqu'à 50 paires clé-valeur de balise.
7. Si vous ajoutez une nouvelle balise portant le même nom de clé qu'une balise existante, la valeur de la nouvelle balise remplace la valeur de la balise existante.
8. Vous pouvez également modifier les valeurs des balises existantes sur cette page.
9. Après avoir ajouté les balises, choisissez Enregistrer les modifications.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment ajouter des balises à un compartiment de répertoire à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;
import software.amazon.awssdk.services.s3control.model.TagResourceResponse;

public class TagResourceExample {
    public static void tagResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                .resourceArn("arn:aws::s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
                .accountId("111122223333")
                .tags(Tag.builder().key("MyTagKey").value("MyTagValue").build())
                .build();

        TagResourceResponse response = s3Control.tagResource(tagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour l'ajout de balises à un compartiment de répertoire, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- TagResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant montre comment ajouter des balises à un bucket de répertoire à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3
 \
--tags "Key=mykey,Value=myvalue"
```

Réponse :

```
{
  "ResponseMetadata": {
      "RequestId": "EXAMPLE123456789",
      "HTTPStatusCode": 200,
      "HTTPHeaders": {
          "date": "Wed, 19 Jun 2025 10:30:00 GMT",
          "content-length": "0"
      },
      "RetryAttempts": 0
  }
}
```

Affichage des balises de bucket du répertoire

Vous pouvez afficher ou répertorier les balises appliquées aux compartiments de répertoire S3. Pour en savoir plus sur les identifications, consultez Utilisation de balises avec des compartiments de répertoire S3.

Autorisations

Pour afficher les balises appliquées à un compartiment de répertoire, vous devez disposer des autorisations suivantes :

- `s3express:ListTagsForResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de répertorier ou d'afficher les balises d'un bucket de répertoire, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des informations nécessaires Autorisations pour afficher ou répertorier les balises du bucket de répertoire.

Étapes

Vous pouvez consulter les balises appliquées aux compartiments d'annuaire à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour afficher les balises appliquées à un compartiment de répertoire à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez des compartiments de répertoire.
3. Choisissez le nom du compartiment.
4. Choisissez l'onglet Propriétés.
5. Accédez à la section Tags pour afficher toutes les balises appliquées au bucket de répertoire.

6. La section Tags affiche les tags définis par l'utilisateur par défaut. Vous pouvez sélectionner l'onglet balises AWS générées pour afficher les balises appliquées à votre compartiment d'annuaire par les AWS services.

En utilisant le AWS SDKs

Cette section fournit un exemple de la manière d'afficher les balises appliquées à un compartiment de répertoire à l'aide du AWS SDKs.

SDK for Java 2.x

Cet exemple montre comment afficher les balises appliquées à un compartiment de répertoire à l'aide du AWS SDK for Java 2.x.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResourceExample {
    public static void listTagsForResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();

        ListTagsForResourceRequest listTagsForResourceRequest =
 ListTagsForResourceRequest.builder()
                .resourceArn("arn:aws::s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
                .accountId("111122223333")
                .build();

        ListTagsForResourceResponse response =
 s3Control.listTagsForResource(listTagsForResourceRequest);
        System.out.println("Tags on my resource:");
        System.out.println(response.toString());
    }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST d'Amazon S3 pour l'affichage des balises appliquées à un compartiment de répertoire, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- ListTagsforResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant vous montre comment afficher les balises appliquées à un bucket de répertoire. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3
 \
```

Réponse : balises présentes :

```
{
  "Tags": [
      {
          "Key": "MyKey1",
          "Value": "MyValue1"
      },
      {
          "Key": "MyKey2",
          "Value": "MyValue2"
      },
      {
          "Key": "MyKey3",
          "Value": "MyValue3"
      }
  ]
```

```
}
```

Réponse : aucun tag n'est présent :

```
{
  "Tags": []
}
```

Supprimer un tag d'un bucket de répertoire

Vous pouvez supprimer des balises des compartiments de répertoire S3. Une AWS balise est une paire clé-valeur qui contient des métadonnées relatives aux ressources, en l'occurrence les compartiments d'annuaire Amazon S3. Pour en savoir plus sur les identifications, consultez Utilisation de balises avec des compartiments de répertoire S3.

> **Note**
>
> Si vous supprimez un tag et apprenez par la suite qu'il était utilisé pour suivre les coûts ou pour contrôler l'accès, vous pouvez le rajouter dans le bucket du répertoire.

Autorisations

Pour supprimer une balise d'un bucket de répertoire, vous devez disposer des autorisations suivantes :

- `s3express:UntagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de supprimer une balise d'un bucket de répertoire, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des conditions requises Autorisations pour supprimer une balise d'un bucket de répertoire.

Étapes

Vous pouvez supprimer des balises des compartiments de répertoire à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour supprimer des balises d'un compartiment de répertoire à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez des compartiments de répertoire.
3. Choisissez le nom du compartiment.
4. Choisissez l'onglet Propriétés.
5. Accédez à la section Tags et cochez la case à côté du tag ou des tags que vous souhaitez supprimer.
6. Sélectionnez Delete (Supprimer).
7. La fenêtre contextuelle Supprimer les balises définies par l'utilisateur apparaît et vous demande de confirmer la suppression de la ou des balises que vous avez sélectionnées.
8. Choisissez Supprimer pour confirmer.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment supprimer des balises d'un bucket de répertoire à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;
import software.amazon.awssdk.services.s3control.model.UntagResourceResponse;

public class UntagResourceExample {
    public static void untagResourceExample() {
        S3ControlClient s3Control =
 S3ControlClient.builder().region(Region.US_WEST_2).build();
```

```
        UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                .resourceArn("arn:aws::s3express:us-west-2:111122223333:bucket/my-
directory-bucket--usw2-az1--x-s3")
                .accountId("111122223333")
                .tagKeys("myTagKey")
                .build();

        UntagResourceResponse response =
 s3Control.untagResource(untagResourceRequest);
        System.out.println("Status code (should be 204):");
        System.out.println(response.sdkHttpResponse().statusCode());
    }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la suppression de balises d'un bucket de répertoire, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- UnTagResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant montre comment supprimer des balises d'un bucket de répertoire à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control untag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3express:us-east-1:444455556666:bucket/prefix--use1-az4--x-s3
 \
--tag-keys "tagkey1" "tagkey2"
```

Réponse :

```
{
  "ResponseMetadata": {
    "RequestId": "EXAMPLE123456789",
    "HTTPStatusCode": 204,
    "HTTPHeaders": {
        "date": "Wed, 19 Jun 2025 10:30:00 GMT",
        "content-length": "0"
    },
    "RetryAttempts": 0
  }
}
```

Utilisation d'Amazon S3 Tables et des compartiments de tables

Amazon S3 Tables fournit un stockage S3 optimisé pour les charges de travail d'analytique, avec des fonctionnalités conçues pour améliorer en permanence les performances des requêtes et réduire les coûts de stockage des tables. La solution S3 Tables est spécialement conçue pour stocker des données tabulaires, telles que des transactions d'achat quotidiennes, des données de capteur diffusées en continu ou des impressions publicitaires. Les données tabulaires représentent des données en colonnes et en lignes, comme dans une table de base de données.

Les données figurant dans S3 Tables sont stockées dans un nouveau type de compartiment : un compartiment de tables, qui stocke les tables en tant que sous-ressources. Les seaux de table permettent de ranger les tables dans Apache Iceberg . À l'aide d'instructions SQL standard, vous pouvez interroger vos tables à l'aide de moteurs de requête compatibles Iceberg, tels qu'Amazon Athena, Amazon Redshift et Apache Spark.

Rubriques

- Fonctionnalités de S3 Tables
- Services connexes
- Didacticiel : Premiers pas avec S3 Tables
- Compartiments de tables
- Maintenance de S3 Tables
- Espaces de noms de tables
- Tables dans des seaux de table S3
- Accès aux données des tables
- Tables S3 Régions AWS, points de terminaison et quotas de service
- Sécurité pour S3 Tables
- Journalisation avec AWS CloudTrail pour les tables S3

Fonctionnalités de S3 Tables

Stockage spécialement conçu pour les tables

Les compartiments de tables S3 sont spécialement conçus pour les tables. Les compartiments de tables offrent un plus grand nombre de transactions par seconde (TPS) et un meilleur débit de requêtes par rapport aux tables autogérées dans les compartiments S3 à usage général. Les compartiments de tables offrent les mêmes durabilité, disponibilité et capacité de mise à l'échelle que les autres types de compartiments Amazon S3.

Support intégré pour Apache Iceberg

Les tables de vos seaux de table sont stockées dans Apache Icebergformat. Vous pouvez interroger ces tables à l'aide du SQL standard dans les moteurs de requête qui prennent en charge Iceberg. Iceberg possède de nombreuses fonctionnalités pour optimiser les performances des requêtes, notamment l'évolution du schéma et l'évolution des partitions.

Avec Iceberg, vous pouvez modifier l'organisation de vos données afin qu'elles puissent évoluer au fil du temps sans avoir à réécrire vos requêtes ou à reconstruire vos structures de données. Iceberg est conçu pour garantir la cohérence et la fiabilité des données grâce à sa prise en charge des transactions. Pour vous aider à corriger des problèmes ou à effectuer des requêtes d'historique, vous pouvez suivre l'évolution des données dans le temps et les restaurer à des versions antérieures.

Optimisation des tables automatisée

Pour optimiser vos tables pour les requêtes, S3 effectue en permanence des opérations de maintenance automatiques, telles que le compactage, la gestion des instantanés et la suppression des fichiers non référencés. Ces opérations améliorent les performances des tables en compactant de petits objets dans des fichiers moins nombreux et plus volumineux. Les opérations de maintenance réduisent également vos coûts de stockage en nettoyant les objets non utilisés. Cette maintenance automatisée rationalise le fonctionnement des lacs de données à grande échelle en réduisant le besoin de maintenance manuelle des tables. Pour chaque table et compartiment de tables, vous pouvez personnaliser les configurations de maintenance.

Gestion des accès et sécurité

Vous pouvez gérer l'accès à la fois aux compartiments de tables et aux tables individuelles à l'aide d' AWS Identity and Access Management (IAM) et des politiques de contrôle des services dans AWS Organizations. S3 Tables utilise un espace de noms de service différent de celui

d'Amazon S3 : l'espace de noms s3tables. Par conséquent, vous pouvez concevoir des politiques spécifiques pour le service S3 Tables et ses ressources. Vous pouvez concevoir des politiques pour accorder l'accès à des tables individuelles, à toutes les tables d'un espace de noms de tables ou à des compartiments de tables entiers. Tous les paramètres de blocage de l'accès public Amazon S3 sont toujours activés pour les compartiments de tables et ne peuvent pas être désactivés.

Intégration aux services AWS d'analyse

Vous pouvez intégrer automatiquement vos compartiments de table Amazon S3 à Amazon SageMaker Lakehouse via la console S3. Cette intégration permet aux services AWS d'analyse de découvrir et d'accéder automatiquement aux données de votre table via le AWS Glue Data Catalog. Après l'intégration, vous pouvez utiliser vos tables à l'aide de services d'analyse tels qu'Amazon Athena, Amazon Redshift QuickSight, etc. Pour plus d'informations sur le fonctionnement de l'intégration, consultezUtilisation d'Amazon S3 Tables avec des services AWS d'analyse.

Services connexes

Vous pouvez utiliser les éléments suivants Services AWS avec les tables S3 pour prendre en charge vos applications d'analyse spécifiques.

- Amazon Athena : Athena est un service de requête interactif qui permet d'analyser les données directement dans Amazon S3 à l'aide du langage SQL standard. Vous pouvez également utiliser Athena pour effectuer des analyses de données de manière interactive en utilisant Apache Spark sans avoir à planifier, configurer ou gérer les ressources. Quand tu cours Apache Spark applications sur Athena, vous soumettez Spark codez pour le traitement et recevez les résultats directement.
- AWS Glue— AWS Glue est un service d'intégration de données sans serveur qui vous permet de découvrir, de préparer, de déplacer et d'intégrer des données provenant de sources multiples. Vous pouvez l'utiliser AWS Glue pour l'analyse, l'apprentissage automatique (ML) et le développement d'applications. AWS Glue inclut également des outils supplémentaires de productivité et d'exploitation des données pour la création, l'exécution de tâches et la mise en œuvre de flux de travail commerciaux.
- Amazon EMR — Amazon EMR est une plate-forme de cluster gérée qui simplifie l'exécution de frameworks de mégadonnées, tels que Apache Hadoop and Apache Spark, AWS pour traiter et analyser de grandes quantités de données.

- Amazon Redshift : Amazon Redshift est un service d'entrepôt de données d'une capacité de plusieurs pétaoctets dans le cloud. Vous pouvez utiliser Amazon Redshift Serverless pour accéder aux données et les analyser sans avoir à recourir à toutes les configurations d'un entrepôt de données provisionné. Les ressources sont automatiquement provisionnées et la capacité de l'entrepôt des données est intelligemment mise à l'échelle afin d'offrir des performances rapides, même pour les charges de travail les plus exigeantes et les plus imprévisibles. Vous ne payez pas de frais lorsque l'entrepôt des données est inactif, vous ne payez donc que ce que vous utilisez. Vous pouvez charger des données et commencer à effectuer des requêtes immédiatement dans l'éditeur de requête Amazon Redshift v2 ou dans votre outil d'informatique décisionnelle (BI) préféré.
- QuickSight— QuickSight est un service d'analyse commerciale permettant de créer des visualisations, d'effectuer des analyses ad hoc et d'obtenir rapidement des informations commerciales à partir de vos données. QuickSight découvre facilement AWS les sources de données et fournit des performances de requête rapides et réactives à l'aide du moteur de calcul QuickSight ultrarapide, parallèle, en mémoire (SPICE).
- AWS Lake Formation— Lake Formation est un service géré qui rationalise le processus de configuration, de sécurisation et de gestion de vos lacs de données. Lake Formation vous aide à détecter vos sources de données, puis à cataloguer, nettoyer et transformer les données. Avec Lake Formation, vous pouvez gérer un contrôle d'accès précis des données de vos lacs de données sur Amazon S3 et de leurs métadonnées dans le AWS Glue Data Catalog.

Didacticiel : Premiers pas avec S3 Tables

Dans ce didacticiel, vous allez créer un compartiment de tables et intégrer des compartiments de tables dans votre région aux services AWS d'analyse. Vous allez ensuite utiliser le AWS CLI pour créer votre premier espace de noms et votre première table dans votre compartiment de tables. Ensuite, vous AWS Lake Formation accordez une autorisation sur votre table, afin de pouvoir commencer à interroger votre table avec Athéna.

> **Tip**
>
> Si vous migrez des données tabulaires de compartiments à usage général vers des compartiments de tables, la bibliothèque de AWS solutions propose une solution guidée pour vous aider. Cette solution automatise le déplacement Apache Hive des tables enregistrées Apache Iceberg AWS Glue Data Catalog et stockées dans des compartiments à usage général vers des compartiments de table en utilisant AWS Step Functions Amazon EMR

avec. Apache Spark Pour plus d'informations, consultez les instructions relatives à la migration de données tabulaires d'Amazon S3 vers des tables S3 dans la bibliothèque de AWS solutions.

Rubriques

- Étape 1 : créer un bucket de tables et l'intégrer aux services AWS d'analyse
- Étape 2 : Création d'un espace de noms de table et d'une table
- (Facultatif) Étape 3 : Accordez les autorisations de Lake Formation sur votre table
- Étape 4 : Interroger des données avec SQL dans Athena

Étape 1 : créer un bucket de tables et l'intégrer aux services AWS d'analyse

Au cours de cette étape, vous utilisez la console Amazon S3 pour créer votre premier compartiment de table. Pour découvrir d'autres méthodes de création d'un compartiment de tables, consultez Création d'un compartiment de tables.

> **Note**
>
> Par défaut, la console Amazon S3 intègre automatiquement vos compartiments de tables à Amazon SageMaker Lakehouse, ce qui permet aux services d' AWS analyse de découvrir et d'accéder automatiquement à vos données de tables S3. Si vous créez votre premier bucket de table par programmation à l'aide de l'API AWS Command Line Interface (AWS CLI) ou REST AWS SDKs, vous devez effectuer manuellement l'intégration des services AWS d'analyse. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon S3 Tables avec des services AWS d'analyse.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer le compartiment de table.
3. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
4. Choisissez Créer un compartiment de tables.

5. Sous Configuration générale, entrez le nom de votre compartiment de table.

   Le nom du compartiment de tables doit présenter les caractéristiques suivantes :

   - Soyez unique pour vous Compte AWS dans la région actuelle.
   - Il doit comporter entre 3 et 63 caractères.
   - Composé uniquement de lettres minuscules, de chiffres et de tirets (). -
   - Il doit commencer et se terminer par une lettre ou un chiffre.

   Une fois que vous avez créé le bucket de table, vous ne pouvez pas modifier son nom. Le bucket Compte AWS qui crée le tableau en est propriétaire. Pour plus d'informations sur la dénomination des compartiments de table, consultezRègles de dénomination des compartiments de tables.
6. Dans la section Intégration aux services AWS d'analyse, assurez-vous que la case Activer l'intégration est cochée.

   Si l'option Activer l'intégration est sélectionnée lorsque vous créez votre premier compartiment de table à l'aide de la console, Amazon S3 tente d'intégrer votre compartiment de table aux services AWS d'analyse. Cette intégration vous permet d'utiliser les services AWS d'analyse pour accéder à toutes les tables de la région actuelle. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon S3 Tables avec des services AWS d'analyse.
7. Choisissez Créer un compartiment.

Étape 2 : Création d'un espace de noms de table et d'une table

Pour cette étape, vous devez créer un espace de noms dans votre compartiment de tables, puis créer une nouvelle table sous cet espace de noms. Vous pouvez créer un espace de noms de table et une table à l'aide de la console ou du AWS CLI.

> **Important**
>
> Lorsque vous créez des tables, assurez-vous d'utiliser toutes les lettres minuscules dans les noms et les définitions de tables. Par exemple, assurez-vous que les noms de vos colonnes sont tous en minuscules. Si le nom ou la définition de votre table contient des majuscules, le tableau n'est pas pris en charge par AWS Lake Formation ou par le AWS Glue Data Catalog.

Dans ce cas, votre table ne sera pas visible par les services d' AWS analyse tels qu'Amazon Athena, même si vos compartiments de tables sont intégrés aux AWS services d'analyse. Si la définition de votre table contient des majuscules, le message d'erreur suivant s'affiche lorsque vous exécutez une `SELECT` requête dans Athena : « GENERIC_INTERNAL_ERROR : Get table request failed : com.amazonaws.services.glue.model. ValidationException: ressource de fédération non prise en charge - Noms de table ou de colonne non valides. »

Utilisation de la console S3 et d'Amazon Athena

La procédure suivante utilise la console Amazon S3 pour créer un espace de noms et une table avec Amazon Athena.

Pour créer un espace de noms de table et une table

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
3. Sur la page Compartiments de table, choisissez le compartiment de table dans lequel vous souhaitez créer une table.
4. Sur la page des détails du compartiment de table, choisissez Create table with Athena.
5. Dans la boîte de dialogue Créer une table avec Athena, choisissez Créer un espace de noms, puis entrez un nom dans le champ Nom de l'espace de noms. Les noms des espaces de noms doivent comporter de 1 à 255 caractères et être uniques dans le compartiment de table. Les caractères valides sont a—z, 0—9 et les traits de soulignement (). _ Les traits de soulignement ne sont pas autorisés au début des noms d'espaces de noms.
6. Choisissez Create namespace (Créer un espace de noms).
7. Choisissez Créer une table avec Athéna.
8. La console Amazon Athena s'ouvre et l'éditeur de requêtes Athena apparaît. L'éditeur de requêtes contient un exemple de requête que vous pouvez utiliser pour créer une table. Modifiez la requête pour spécifier le nom de la table et les colonnes que vous souhaitez attribuer à votre table.
9. Lorsque vous avez terminé de modifier la requête, choisissez Exécuter pour créer votre table.

Si la création de votre table a réussi, le nom de votre nouvelle table apparaît dans la liste des tables d'Athena. Lorsque vous revenez à la console Amazon S3, votre nouvelle table apparaît dans la liste des tables de la page de détails de votre compartiment de tables une fois que vous l'avez actualisée.

À l'aide du AWS CLI

Pour utiliser les AWS CLI exemples de commandes suivants afin de créer un espace de noms dans votre compartiment de tables, puis de créer une nouvelle table avec un schéma sous cet espace de noms, remplacez les *`user input placeholder`* valeurs par les vôtres.

Prérequis

- Associez la `AmazonS3TablesFullAccess`politique à votre identité IAM.
- Installez AWS CLI la version 2.23.10 ou supérieure. Pour plus d'informations, consultez Installation ou mise à jour de la version la plus récente de l' AWS CLI (langue française non garantie) dans le Guide de l'utilisateur AWS Command Line Interface .

1. Créez un nouvel espace de noms dans votre compartiment de table en exécutant la commande suivante :

   ```
   aws s3tables create-namespace \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
   --namespace my_namespace
   ```

   - Vérifiez que votre espace de noms a bien été créé en exécutant la commande suivante :

     ```
     aws s3tables list-namespaces \
     --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket
     ```

2. Créez une nouvelle table avec un schéma de table en exécutant la commande suivante :

   ```
   aws s3tables create-table --cli-input-json file://mytabledefinition.json
   ```

   Pour le `mytabledefinition.json` fichier, utilisez l'exemple de définition de table suivant :

   ```
   {
       "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
   ```

```
    "namespace": "my_namespace",
    "name": "my_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                     {"name": "id", "type": "int","required": true},
                     {"name": "name", "type": "string"},
                     {"name": "value", "type": "int"}
                ]
            }
        }
    }
}
```

(Facultatif) Étape 3 : Accordez les autorisations de Lake Formation sur votre table

Pour cette étape, vous accordez des autorisations Lake Formation sur votre nouvelle table à d'autres responsables IAM. Ces autorisations permettent à des personnes autres que vous d'accéder aux ressources des tables à l'aide d'Athena et AWS d'autres services d'analyse. Pour de plus amples informations, veuillez consulter Octroi d'une autorisation sur une table ou une base de données. Si vous êtes le seul utilisateur à accéder à vos tables, vous pouvez ignorer cette étape.

1. Ouvrez la AWS Lake Formation console sur https://console.aws.amazon.com/lakeformation/ et connectez-vous en tant qu'administrateur du lac de données. Pour plus d'informations sur la création d'un administrateur de lac de données, voir Création d'un administrateur de lac de données.
2. Dans le volet de navigation, choisissez Autorisations de données, puis Accorder.
3. Sur la page Accorder des autorisations, sous Principaux, sélectionnez Utilisateurs et rôles IAM, puis choisissez l'utilisateur ou le rôle IAM que vous souhaitez autoriser à exécuter des requêtes sur votre table.
4. Sous Balises LF ou ressources de catalogue, choisissez Ressources de catalogue de données nommées.
5. Procédez de l'une des manières suivantes, selon que vous souhaitez accorder l'accès à toutes les tables de votre compte ou uniquement aux ressources du compartiment de tables que vous avez créé :

- Pour les catalogues, choisissez le catalogue au niveau du compte que vous avez créé lorsque vous avez intégré votre compartiment de table. Par exemple, *111122223333*:s3tablescatalog.
- Pour les catalogues, choisissez le sous-catalogue de votre compartiment de table. Par exemple, *111122223333*:s3tablescatalog/*amzn-s3-demo-table-bucket*.

6. (Facultatif) Si vous avez choisi le sous-catalogue pour votre compartiment de tables, effectuez l'une des opérations suivantes ou les deux :
   - Pour les bases de données, choisissez l'espace de noms de compartiments de table que vous avez créé.
   - Pour Tables, choisissez la table que vous avez créée dans votre bucket de tables, ou choisissez Toutes les tables.
7. Selon que vous avez choisi un catalogue ou un sous-catalogue et selon que vous avez ensuite choisi une base de données ou une table, vous pouvez définir des autorisations au niveau du catalogue, de la base de données ou de la table. Pour plus d'informations sur les autorisations de Lake Formation, consultez la section Gestion des autorisations de Lake Formation dans le Guide du AWS Lake Formation développeur.

   Effectuez l'une des actions suivantes :
   - Pour les autorisations du catalogue, choisissez Super pour accorder à l'autre principal toutes les autorisations sur votre catalogue, ou choisissez des autorisations plus détaillées, telles que Describe.
   - Pour les autorisations de base de données, vous ne pouvez pas choisir Super pour accorder à l'autre principal toutes les autorisations sur votre base de données. Choisissez plutôt des autorisations plus détaillées, telles que Describe.
   - Pour les autorisations de table, choisissez Super pour accorder à l'autre principal toutes les autorisations sur votre table, ou choisissez des autorisations plus détaillées, telles que Select ou Describe.

   > **Note**
   >
   > Lorsque vous accordez des autorisations sur une ressource du catalogue de données à un compte externe ou directement à un responsable IAM d'un autre compte, Lake Formation utilise le service AWS Resource Access Manager (AWS RAM) pour partager la ressource. Si le compte du bénéficiaire appartient à la même organisation que le compte du donateur, la ressource partagée est immédiatement

accessible au bénéficiaire. Si le compte du bénéficiaire n'appartient pas à la même organisation, AWS RAM envoie une invitation au compte du bénéficiaire pour qu'il accepte ou rejette la subvention de ressources. Ensuite, pour rendre la ressource partagée disponible, l'administrateur du lac de données du compte bénéficiaire doit utiliser la AWS RAM console ou AWS CLI accepter l'invitation. Pour plus d'informations sur le partage de données entre comptes, voir Partage de données entre comptes dans Lake Formation dans le guide du AWS Lake Formation développeur.

8. Choisissez Accorder.

Étape 4 : Interroger des données avec SQL dans Athena

Vous pouvez interroger votre table avec SQL dans Athena. Athena prend en charge les requêtes DDL (Data Definition Language), DML (Data Manipulation Language) et DQL (Data Query Language) pour les tables S3.

Vous pouvez accéder à la requête Athena depuis la console Amazon S3 ou via la console Amazon Athena.

Utilisation de la console S3 et d'Amazon Athena

La procédure suivante utilise la console Amazon S3 pour accéder à l'éditeur de requêtes Athena afin que vous puissiez interroger une table avec Amazon Athena.

Pour interroger une table

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
3. Sur la page Compartiments de table, choisissez le compartiment de table contenant la table que vous souhaitez interroger.
4. Sur la page des détails du bucket de table, cliquez sur le bouton d'option situé à côté du nom de la table que vous souhaitez interroger.
5. Choisissez Query table with Athena.

6. La console Amazon Athena s'ouvre et l'éditeur de requêtes Athena apparaît avec un exemple `SELECT` de requête chargé pour vous. Modifiez cette requête en fonction de votre cas d'utilisation.
7. Pour exécuter la requête, choisissez ensuite Run (Exécuter).

Utilisation de la console Amazon Athena

Pour interroger une table

1. Ouvrez la console à l'adresse https://console.aws.amazon.com/athena/.
2. Interrogez votre table. Voici un exemple de requête que vous pouvez modifier. Veillez à remplacer les *`user input placeholders`* par vos propres informations.

```
SELECT * FROM "s3tablescatalog/amzn-s3-demo-table-bucket"."my_namespace"."my_table"
 LIMIT 10
```

3. Pour exécuter la requête, choisissez ensuite Run (Exécuter).

Compartiments de tables

Les compartiments de tables Amazon S3 sont un type de compartiment S3 que vous pouvez utiliser pour créer et stocker des tables en tant que ressources S3. Les compartiments de tables permettent de stocker les données tabulaires et les métadonnées sous forme d'objets qui peuvent être utilisés dans les charges de travail d'analytique. S3 effectue automatiquement la maintenance de vos compartiments de tables afin de réduire les coûts de stockage de vos tables. Pour de plus amples informations, veuillez consulter Maintenance de S3 Tables.

Pour interagir avec les tables stockées dans vos compartiments de tables, vous pouvez intégrer ces derniers avec des applications d'analytique prenant en charge Apache Iceberg. Les compartiments de table s'intègrent aux services AWS d'analyse via le AWS Glue Data Catalog. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon S3 Tables avec des services AWS d'analyse. Vous pouvez également interagir avec vos tables à l'aide de moteurs de requêtes open source utilisant le catalogue de tables Amazon S3 pourApache Iceberg. Pour de plus amples informations, veuillez consulter Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison.

Chaque compartiment de tables possède un Amazon Resource Name (ARN) unique et une politique de ressources qui lui est attachée. Le compartiment de table ARNs suit le format suivant :

```
arn:aws:s3tables:Region:OwnerAccountID:bucket/bucket-name
```

Tous les compartiments de tables et toutes les tables sont privés et ne peuvent pas être rendus publics. Ces ressources sont accessibles uniquement par les utilisateurs auxquels l'accès a été accordé explicitement. Pour accorder l'accès, vous pouvez utiliser des politiques basées sur les ressources IAM pour les compartiments de tables et les tables, et des politiques basées sur l'identité IAM pour les utilisateurs et les rôles.

Par défaut, vous pouvez créer jusqu'à 10 compartiments de table par Région AWS personne. Compte AWS Pour demander une augmentation de quota pour les compartiments de tables ou les tables, contactez Support.

Types de seaux de table

Amazon S3 prend en charge les types de compartiments de table suivants :

Seaux de table gérés par le client

Les compartiments de tables gérés par le client sont des ressources permettant de stocker les tables Amazon S3 créées et gérées par les clients. Vous créez ces compartiments de manière explicite, vous choisissez leurs noms et vous gardez le contrôle total sur les tables et les espaces de noms qu'ils contiennent. Pour les compartiments de table gérés par le client, vous pouvez créer, supprimer, définir un chiffrement par défaut personnalisé ou configurer les options de maintenance selon vos besoins.

AWS seaux de table gérés

AWS les compartiments de tables AWS gérés sont des ressources gérées qui stockent automatiquement les tables créées par les AWS services, telles que l'inventaire en temps réel et les tables de journal créées par S3 Metadata. Ces compartiments fournissent un emplacement centralisé pour toutes les tables générées par le système. Ces compartiments suivent une convention de dénomination standard, utilisent un espace de noms standard pour toutes les tables et ont des configurations de maintenance et de chiffrement par défaut prédéfinies que S3 modifie en votre nom. Vous disposez d'un accès en lecture seule pour interroger les données, tout en AWS gérant toutes les opérations de création, de mise à jour et de maintenance des tables. Pour de plus amples informations, veuillez consulter Utilisation de compartiments de table AWS gérés.

Il existe plusieurs types de compartiments Amazon S3. Avant de créer un bucket, assurez-vous de choisir le type de bucket qui correspond le mieux à votre application et à vos exigences de performance. Pour plus d'informations sur les différents types de bucket et les cas d'utilisation appropriés pour chacun, consultezCompartiments.

Rubriques

- Règles de dénomination des compartiments de tables, des tables et des espaces de noms Amazon S3
- Création d'un compartiment de tables
- Suppression d'un compartiment de tables
- Affichage des détails d'un compartiment de tables Amazon S3
- Gestion des politiques de compartiments de tables
- Utilisation de compartiments de table AWS gérés

Règles de dénomination des compartiments de tables, des tables et des espaces de noms Amazon S3

Lorsque vous créez un bucket de table, vous choisissez un nom de Région AWS bucket qui doit être unique pour votre compte dans la région choisie. Une fois que vous avez créé un bucket de table, vous ne pouvez pas modifier le nom ou la région du bucket. Les noms des compartiments de tables doivent suivre des règles de dénomination spécifiques. Pour plus d'informations sur les règles de dénomination des compartiments de tables, ainsi que des tables et des espaces de noms qu'ils contiennent, consultez la rubrique suivante.

Rubriques

- Règles de dénomination des compartiments de tables
- Règles de dénomination des tables et des espaces de noms

Règles de dénomination des compartiments de tables

Lorsque vous créez des compartiments de tables Amazon S3, vous spécifiez un nom de compartiment de tables. Comme les autres types de compartiments, les compartiments de tables ne peuvent pas être renommés. Contrairement aux autres types de compartiments, les compartiments de table ne se trouvent pas dans un espace de noms global. Chaque nom de compartiment de votre compte doit donc être unique uniquement dans votre région actuelle AWS .

Pour connaître les règles de dénomination des compartiments à usage général, consultez Règles de dénomination des compartiments à usage général. Pour les règles de dénomination des compartiments de répertoires, consultez Règles de dénomination des compartiments de répertoires.

Les règles de dénomination suivantes s'appliquent pour les compartiments de tables.

- Les noms de compartiment peuvent comporter entre 3 et 63 caractères.
- Les noms de compartiments ne peuvent être composés que de lettres minuscules, de chiffres et de traits d'union (). -
- Les noms de compartiment doivent commencer et se terminer par une lettre ou un chiffre.
- Les noms des compartiments ne doivent pas contenir de soulignement (_) ni de point (.).
- Les noms de compartiments ne doivent pas commencer par l'un des préfixes réservés suivants :
  - `xn--`
  - `sthree-`
  - `amzn-s3-demo-`
  - `aws`
- Les noms des compartiments ne doivent pas se terminer par l'un des suffixes réservés suivants :
  - `-s3alias`
  - `--ol-s3`
  - `--x-s3`
  - `--table-s3`

Règles de dénomination des tables et des espaces de noms

Les règles de dénomination suivantes s'appliquent aux tables et aux espaces de noms contenus dans des compartiments de tables :

- Les noms doivent comporter entre 1 et 255 caractères.
- Les noms ne peuvent être composés que de lettres minuscules, de chiffres et de traits de soulignement (). _ Les traits de soulignement ne sont pas autorisés au début ou à la fin des noms d'espaces de noms.
- Les noms doivent commencer et se terminer par une lettre ou un chiffre.
- Les noms ne doivent pas contenir de tirets (-) ni de points (.).
- Le nom d'une table doit être unique au sein d'un espace de noms.

- Un espace de noms doit être unique dans un compartiment de tables.
- Les noms d'espaces de noms ne doivent pas commencer par le préfixe `aws` réservé.

Création d'un compartiment de tables

Les compartiments de tables Amazon S3 sont un type de compartiment S3 que vous pouvez utiliser pour créer et stocker des tables en tant que ressources S3. Pour commencer à utiliser S3 Tables, vous devez créer un compartiment de tables dans lequel stocker et gérer les tables. Lorsque vous créez un bucket de table, vous choisissez un nom de bucket et Région AWS. Le nom du bucket de table doit être unique pour votre compte dans la région choisie. Une fois que vous avez créé un bucket de table, vous ne pouvez pas modifier le nom ou la région du bucket. Pour obtenir des informations sur la dénomination des compartiment de tables, consultez Règles de dénomination des compartiments de tables, des tables et des espaces de noms Amazon S3.

Les compartiment de tables possèdent le format d'Amazon Resource Name (ARN) suivant :

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name
```

Par défaut, vous pouvez créer jusqu'à 10 compartiments de table par région dans un Compte AWS. Pour demander une augmentation de quota pour les compartiments de tables ou les tables, contactez Support.

Lorsque vous créez un compartiment de tables, vous pouvez spécifier le type de chiffrement qui sera utilisé pour chiffrer les tables que vous créez dans ce compartiment. Pour plus d'informations sur les options de chiffrement des compartiments, consultezthe section called "Chiffrement".

Conditions préalables à la création de compartiments de table

Pour créer un bucket de table, vous devez d'abord effectuer les opérations suivantes :

- Assurez-vous que vous disposez des autorisations AWS Identity and Access Management (IAM) pours3tables:CreateTableBucket.

> **Note**
>
> Si vous choisissez SSE-KMS comme type de chiffrement par défaut, vous devez disposer d'autorisations et d'autorisations pour `s3tables:PutTableBucketEncryption` la

clé choisie AWS KMS . `DescribeKey` En outre, la AWS KMS clé que vous utilisez doit autoriser S3 Tables à effectuer la maintenance automatique des tables. Pour de plus amples informations, consultez Exigences d'autorisation pour le chiffrement SSE-KMS des tables S3.

Pour créer un bucket de table, vous pouvez utiliser la console Amazon S3, l'API REST Amazon S3, AWS Command Line Interface (AWS CLI) ou AWS SDKs.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.
3. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
4. Choisissez Créer un compartiment de tables pour ouvrir la page Créer un compartiment de tables.
5. Sous Propriétés, entrez un nom pour votre compartiment de tables.

   Le nom du compartiment de tables doit présenter les caractéristiques suivantes :

   - Il doit être unique pour votre compte dans la région actuelle.
   - Il doit comporter entre 3 et 63 caractères.
   - Il doit être composé uniquement de lettres minuscules, de chiffres et de traits d'union (-).
   - Il doit commencer et se terminer par une lettre ou un chiffre.

   Une fois le compartiment créé, vous ne pouvez pas changer son nom. Celui Compte AWS qui crée le bucket en est propriétaire. Pour obtenir des informations sur la dénomination des compartiment de tables, consultez Règles de dénomination des compartiments de tables, des tables et des espaces de noms Amazon S3.
6. Si vous souhaitez intégrer vos compartiments de table aux services AWS d'analyse, assurez-vous que l'option Activer l'intégration est sélectionnée sous Intégration aux services AWS d'analyse.

> **Note**
>
> Lorsque vous créez votre premier compartiment de table à l'aide de la console avec l'option Activer l'intégration sélectionnée, Amazon S3 tente d'intégrer automatiquement votre compartiment de table aux services AWS d'analyse. Cette intégration vous permet d'utiliser les services AWS d'analyse pour interroger toutes les tables de la région actuelle. Pour de plus amples informations, veuillez consulter Utilisation d'Amazon S3 Tables avec des services AWS d'analyse.

7. Pour configurer le chiffrement par défaut, dans Type de chiffrement, choisissez l'une des options suivantes :

   - Chiffrement côté serveur avec clé gérée Amazon S3 (SSE-S3)
   - Chiffrement côté serveur avec AWS Key Management Service clé (SSE-KMS)

   Pour plus d'informations sur les options de chiffrement des données de table, consultezProtection des données des tables S3 grâce au chiffrement.
8. Choisissez Créer un compartiment.

En utilisant le AWS CLI

Cet exemple montre comment créer un compartiment de tables à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3tables create-table-bucket \
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
```

Par défaut, les compartiments de table S3 utilisent SSE-S3 comme paramètre de chiffrement par défaut, mais vous pouvez utiliser le `--encryption-configuration` paramètre facultatif pour spécifier un autre type de chiffrement. Les exemples suivants montrent comment créer un compartiment qui utilise le chiffrement SSE-KMS. Pour plus d'informations sur les paramètres de chiffrement des compartiments de table, consultezProtection des données des tables S3 grâce au chiffrement.

```
aws s3tables create-table-bucket \
```

```
    --region us-east-2 \
    --name amzn-s3-demo-bucket1
    --encryption-configuration '{
                    "sseAlgorithm": "aws:kms",
                    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab" }'
```

Suppression d'un compartiment de tables

Vous pouvez utiliser Amazon S3 APIs AWS Command Line Interface, ou AWS SDKs pour supprimer un bucket de table. Avant de supprimer un compartiment de tables, vous devez supprimer tous les espaces de noms et toutes les tables qu'il contient.

En utilisant le AWS CLI

Cet exemple montre comment supprimer un compartiment de tables à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3tables delete-table-bucket \
    --region us-east-2 \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1
```

Affichage des détails d'un compartiment de tables Amazon S3

Vous pouvez consulter les détails d'un compartiment de tables Amazon S3 par programmation à l'aide de l'API REST S3 Tables, AWS CLI ou. AWS SDKs

À l'aide du AWS CLI

Cet exemple montre comment obtenir des détails sur un compartiment de tables à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3tables get-table-bucket --table-bucket-arn arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Gestion des politiques de compartiments de tables

Vous pouvez ajouter, supprimer, mettre à jour et consulter les politiques de compartiment pour les compartiments de tables Amazon S3 à l'aide de l'API REST Amazon S3 et du AWS Command Line Interface (AWS CLI). AWS SDKs Pour plus d'informations, consultez les rubriques suivantes.

Pour plus d'informations, consultez les rubriques suivantes. Pour plus d'informations sur les actions AWS Identity and Access Management (IAM) et les clés de condition prises en charge pour les tables Amazon S3, consultezGestion des accès pour S3 Tables. Pour voir des exemples de politiques de compartiments pour les compartiments de tables, consultez Politiques basées sur les ressources pour S3 Tables.

Ajout d'une politique de compartiment de tables

Pour ajouter une politique de bucket à un bucket de table, utilisez l' AWS CLI exemple suivant.

À l'aide du AWS CLI

Cet exemple montre comment créer une politique de compartiment de tables à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez-la *user input placeholders* par vos propres informations.

```
aws s3tables put-table-bucket-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1  \
    --resource-policy your-policy-JSON
```

Consultation d'une politique de compartiment de tables

Pour consulter la politique de bucket attachée à un bucket de table, utilisez l' AWS CLI exemple suivant.

À l'aide du AWS CLI

Cet exemple montre comment afficher la politique attachée à un bucket de table à l'aide du AWS CLI. Pour utiliser la commande, remplacez-la *user input placeholders* par vos propres informations.

```
aws s3tables get-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Suppression d'une politique de compartiment de tables

Pour supprimer une politique de bucket attachée à un bucket de table, utilisez l' AWS CLI exemple suivant.

À l'aide du AWS CLI

Cet exemple montre comment supprimer une politique de compartiment de tables à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez-la *`user input placeholders`* par vos propres informations.

```
aws s3tables delete-table-bucket-policy --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1
```

Utilisation de compartiments de table AWS gérés

AWS les compartiments de table gérés sont des compartiments de table S3 spécialisés conçus pour stocker des tables AWS gérées, telles que les tables de Accélération de la découverte des données avec les métadonnées S3 journal et d'inventaire en temps réel. Contrairement aux compartiments de tables gérés par le client que vous créez et gérez directement, les compartiments de tables AWS gérés sont automatiquement provisionnés AWS lorsque vous configurez des fonctionnalités qui nécessitent des tables gérées. AWS Lorsque des tables gérées sont créées, elles appartiennent à un espace de noms prédéfini basé sur le compartiment source qui ne peut pas être modifié. Chaque AWS compte possède un compartiment de tables AWS géré par région, conformément à la convention de dénomination`aws-s3`. Ce compartiment sert d'emplacement centralisé pour toutes les tables gérées associées aux ressources de votre compte dans cette région.

Le tableau suivant compare les compartiments de table AWS gérés avec les compartiments de table gérés par le client.

Fonctionnalité	AWS seaux de table gérés	Seaux de table gérés par le client
Création	Créé automatiquement par les AWS services	Vous les créez manuellement
Nommage	Utiliser une convention de dénominat ion standard (aws-s3)	Vous définissez vos propres noms

Fonctionnalité	AWS seaux de table gérés	Seaux de table gérés par le client
Création de tables	Seuls AWS les services peuvent créer des tables	Vous pouvez créer des tables
Contrôle de l'espace de noms	Impossible de créer ou de supprimer des espaces de noms (toutes les tables appartiennent à un espace de noms fixe)	Vous pouvez créer et supprimer des espaces de noms
Accès	Accès en lecture seule	Accès complet à
Chiffrement	Vous ne pouvez modifier les paramètres de chiffrement par défaut (SSE-S3) que si vous avez chiffré la table initiale avec une clé gérée AWS KMS par le client.	Vous pouvez définir le chiffrement par défaut au niveau du compartim ent et le modifier à tout moment
Maintenance	Géré par les AWS services	La maintenance automatisée peut être personnalisée au niveau du godet

Autorisations pour créer des AWS compartiments de tables gérés

Pour utiliser des compartiments de tables AWS gérés, vous devez disposer des autorisations nécessaires pour créer des compartiments et des tables AWS gérés, spécifier les paramètres de chiffrement pour les tables AWS gérées ainsi que les autorisations de lecture de base pour interroger les tables.

Voici un exemple de politique qui vous permettra de créer un bucket de table AWS géré via des configurations de service :

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"PermissionsToWorkWithMetadataTables",
         "Effect":"Allow",
         "Action":[
```

```
                "s3:CreateBucketMetadataTableConfiguration",
                "s3tables:CreateTableBucket",
                "s3tables:CreateNamespace",
                "s3tables:CreateTable",
                "s3tables:GetTable",
                "s3tables:PutTablePolicy"
                "s3tables:PutTableEncryption",
                "kms:DescribeKey"
            ],
            "Resource":[
               "arn:aws:s3:::bucket/amzn-s3-demo-source-bucket",
               "arn:aws:s3tables:region:111122223333:bucket/aws-s3",
               "arn:aws:s3tables:region:111122223333:bucket/aws-s3/table/*"
            ]
         }
      ]
}
```

Voici un exemple de politique qui vous permettra d'interroger des tables dans des compartiments de tables AWS gérés :

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"PermissionsToWorkWithMetadataTables",
         "Effect":"Allow",
         "Action":[
             "s3tables:GetTable",
             "s3tables:GetTableData",
             "s3tables:GetTableMetadataLocation",
             "kms:Decrypt"
         ],
         "Resource":[
            "arn:aws:s3tables:region:111122223333:bucket/aws-s3",
            "arn:aws:s3tables:region:111122223333:bucket/aws-s3/table/*"
         ]
      }
   ]
}
```

Interrogation de tables dans des compartiments de tables AWS gérés

Vous pouvez interroger des tables AWS gérées dans des compartiments de tables AWS gérés à l'aide de méthodes d'accès et de moteurs pris en charge par S3 Tables. Voici quelques exemples de requêtes :

Using standard SQL

L'exemple suivant montre comment interroger des tables AWS gérées à l'aide de la syntaxe SQL standard.

```
SELECT *
FROM "s3tablescatalog/aws-s3"."b_amzn-s3-demo-source-bucket"."inventory"
LIMIT 10;
```

L'exemple suivant montre comment joindre des tables AWS gérées à vos propres tables.

```
SELECT *
FROM "s3tablescatalog/aws-s3"."b_amzn-s3-demo-source-bucket"."inventory" a
JOIN "s3tablescatalog/amzn-s3-demo-table-bucket"."my_namespace"."my_table" b
ON a.key = b.key
LIMIT 10;
```

Using Spark

L'exemple suivant montre comment interroger votre table avecSpark.

```
spark.sql("""
    SELECT *
    FROM ice_catalog.inventory a
    JOIN ice_catalog.my_table b
    ON a.key = b.key
""").show(10, true)
```

L'exemple suivant montre comment joindre votre table AWS gérée à une autre table.

```
SELECT *
FROM inventory a
JOIN my_table b
ON a.key = b.key
```

```
LIMIT 10;
```

Chiffrement pour les AWS compartiments de tables gérés

Par défaut, les compartiments de tables AWS gérés sont chiffrés par chiffrement côté serveur à l'aide de clés gérées Amazon S3 (SSE-S3). Une fois votre bucket de table AWS géré créé, vous pouvez l'utiliser PutTableBucketEncryptionpour définir le paramètre de chiffrement par défaut du bucket afin d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS).

Lors de la création de vos tables AWS gérées, vous pouvez choisir de les chiffrer avec SSE-KMS. Si vous choisissez d'utiliser SSE-KMS, vous devez fournir une clé KMS gérée par le client dans la même région que votre bucket de table AWS géré. Vous pouvez définir le type de chiffrement pour vos tables AWS gérées uniquement lors de leur création. Une fois qu'une table AWS gérée est créée, vous ne pouvez pas modifier ses paramètres de chiffrement.

Si vous souhaitez que le compartiment de table AWS géré et les tables qui y sont stockées utilisent la même clé KMS, assurez-vous d'utiliser la même clé KMS que celle que vous avez utilisée pour chiffrer vos tables afin de chiffrer votre compartiment de tables après sa création. Une fois que vous avez modifié les paramètres de chiffrement par défaut pour votre compartiment de tables afin d'utiliser SSE-KMS, ces paramètres de chiffrement sont utilisés pour toutes les futures tables créées dans le compartiment.

Maintenance de S3 Tables

Amazon S3 effectue automatiquement la maintenance afin d'améliorer les performances de vos tables dans des compartiments de tables S3. La maintenance est effectuée au niveau du godet de la table individuelle et comprend les éléments suivants :

Maintenance au niveau du godet de table :

- Suppression des fichiers non référencés : nettoie les fichiers orphelins pour optimiser l'utilisation et les coûts du stockage

Maintenance au niveau de la table :

- Compaction des fichiers : consolide les petits fichiers pour améliorer les performances des requêtes et réduire les coûts de stockage.
- Gestion des instantanés : contrôle l'historique des versions des tables et empêche la croissance excessive des métadonnées.

Ces options sont activées par défaut. Vous pouvez modifier ou désactiver ces opérations via les fichiers de configuration de maintenance.

Rubriques

- Statut des tâches de maintenance de S3 Tables
- Entretien des seaux de table
- Entretien des tables
- Considérations et restrictions relatives aux tâches de maintenance

Statut des tâches de maintenance de S3 Tables

Les tâches de maintenance de S3 Tables s'exécutent régulièrement pour vos tables ou compartiments de tables S3. Vous pouvez interroger le statut de ces tâches à l'aide de l'API `GetTableMaintenanceJobStatus`.

Pour connaître l'état de vos tâches de maintenance à l'aide du AWS CLI

L'exemple suivant permet d'obtenir les statuts des tâches de maintenance à l'aide de l'API `GetTableMaintenanceJobStatus`.

```
aws s3tables get-table-maintenance-job-status \
   --table-bucket-arn="arn:aws:s3tables:arn:aws::111122223333:bucket/amzn-s3-demo-bucket1" \
   --namespace="mynamespace" \
   --name="testtable"
```

Pour plus d'informations, consultez get-table-maintenance-job-status dans la Référence des commandes de l'AWS CLI .

Les tâches de maintenance de S3 Tables peuvent évoluer entre quatre statuts possibles :

- `Successful`
- `Failed`
- `Disabled`
- `Not_Yet_Run`

Les tâches dont le statut a échoué incluront un message d'échec. La liste suivante décrit les messages d'échec possibles.

- Exception de validation Iceberg rencontrée lors de la tentative de lecture de la table. Assurez-vous que votre table est lisible, qu'elle respecte la spécification Iceberg et qu'elle ne contient que des chemins S3 commençant par votre alias de table S3.
- La gestion des instantanés d'Iceberg ne prend actuellement pas en charge les balises ou les références définies par l'utilisateur.
- La configuration de maintenance des tables Iceberg est incompatible avec « history.expire ». max-snapshot-age-ms' et « history.expire ». min-snapshots-to-keep' propriétés du tableau.
- La gestion des instantanés Iceberg et la suppression de fichiers non référencés ne sont pas prises en charge lorsque la propriété de table « gc.enabled » est fausse. Assurez-vous que cette propriété n'est pas définie ou qu'elle est explicitement définie sur true.
- Impossible de valider car les métadonnées ne sont pas à jour. La maintenance sera réessayée dès que l'occasion se présentera.
- Accès insuffisant pour effectuer la maintenance de la table. Assurez-vous que la clé utilisée pour chiffrer la table est active, existe et dispose d'une politique de ressources accordant l'accès au principal `maintenance.s3tables.amazonaws.com` du service S3.

  > **Note**
  >
  > Pour plus d'informations sur AWS KMS les autorisations pour les tables S3, consultezExigences d'autorisation pour le chiffrement SSE-KMS des tables S3.

- Erreur interne

Entretien des seaux de table

Amazon S3 propose des opérations de maintenance pour améliorer la gestion et les performances de vos compartiments de table. L'option suivante est activée par défaut pour tous les compartiments de tables. Vous pouvez modifier ou désactiver cette option en spécifiant un fichier de configuration de maintenance pour votre compartiment de tables.

La modification de cette configuration nécessite l'autorisation `s3tables:PutTableBucketMaintenanceConfiguration`.

Rubriques

- Suppression des fichiers non référencés
- Considérations et restrictions

Suppression des fichiers non référencés

La suppression des fichiers non référencés identifie et supprime tous les objets qui ne sont référencés par aucun instantané de table. Dans le cadre de votre politique de suppression de fichiers non référencés, vous pouvez configurer deux propriétés : `unreferencedDays` (3 jours par défaut) et `nonCurrentDays` (10 jours par défaut).

Pour tout objet non référencé par votre table et plus ancien que la propriété `unreferencedDays`, S3 marque l'objet comme non actuel. S3 supprime les objets non actuels après le nombre de jours spécifié par la propriété `nonCurrentDays`.

> **Note**
>
> Les suppressions des objets non actuels sont permanentes et il n'est pas possible de récupérer ces objets.

Pour consulter ou récupérer des objets marqués comme non actuels, vous devez contacter AWS Support. Pour plus d'informations sur la prise de contact AWS Support, consultez la section Contact AWS ou la AWS Support documentation.

La suppression des fichiers non référencés détermine les objets à supprimer de votre table en référence uniquement à cette table. Aucune référence faite à ces objets en dehors de la table n'empêchera la fonctionnalité de suppression des fichiers non référencés de supprimer un objet.

Si vous désactivez la suppression des fichiers non référencés, les tâches en cours ne seront pas affectées. La nouvelle configuration prendra effet pour la prochaine tâche après la modification de la configuration. Pour plus d'informations, consultez les informations de tarification dans Tarification Amazon S3.

Vous ne pouvez configurer la suppression des fichiers non référencés qu'au niveau du compartiment de tables. Cette configuration s'appliquera à chaque table figurant dans votre compartiment.

Pour configurer la suppression de fichiers non référencés à l'aide du AWS CLI

L'exemple suivant définit le paramètre `unreferencedDays` sur 4 jours et le paramètre `nonCurrentDays` sur 10 jours à l'aide de l'API `PutTableBucketMaintenanceConfiguration`.

```
aws s3tables put-table-bucket-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergUnreferencedFileRemoval \
   --value '{"status":"enabled","settings":{"icebergUnreferencedFileRemoval":
{"unreferencedDays":4,"nonCurrentDays":10}}}'
```

Pour plus d'informations, consultez put-table-bucket-maintenance-configuration dans la Référence des commandes de l'AWS CLI .

Considérations et restrictions

Pour en savoir plus sur les considérations supplémentaires et les limites relatives à la suppression des fichiers non référencés, consultez the section called "Considérations et restrictions".

Entretien des tables

S3 Tables propose des opérations de maintenance pour améliorer la gestion et les performances de vos tables individuelles. Les options suivantes sont activées par défaut pour toutes les tables contenues dans des compartiments de tables. Vous pouvez modifier ou désactiver ces options en spécifiant des fichiers de configuration de maintenance pour votre table S3.

La modification de cette configuration nécessite les autorisations `s3tables:GetTableMaintenanceConfiguration` et `s3tables:PutTableMaintenanceConfiguration`.

Rubriques

- Compactage
- Gestion des instantanés
- Considérations et restrictions

Compactage

Le compactage est configuré au niveau de la table et combine plusieurs petits objets en objets moins nombreux et plus grands afin d'améliorer les performances des Apache Iceberg requêtes. Lorsque vous combinez des objets, le compactage applique également les effets des suppressions au niveau des lignes dans votre tableau.

Le compactage est activé par défaut pour toutes les tables, avec une taille de fichier cible par défaut de 512 Mo ou une valeur personnalisée que vous spécifiez entre 64 Mo et 512 Mo. Les fichiers compactés sont écrits sous la forme de l'instantané le plus récent de votre table.

> **Note**
>
> Le compactage est pris en charge sur Apache Parquet les types de ORC fichiersAvro, et.

Stratégies de compactage

Vous pouvez choisir parmi plusieurs stratégies de compactage susceptibles d'améliorer encore les performances des requêtes en fonction de vos modèles de requêtes et de l'ordre de tri des tables.

S3 Tables prend en charge les stratégies de compactage suivantes pour les tables :

- Auto (par défaut)
  - Amazon S3 sélectionne la meilleure stratégie de compactage en fonction de l'ordre de tri de votre table. Il s'agit de la stratégie de compactage par défaut pour toutes les tables.
  - Pour les tables dont l'ordre de tri est défini dans leurs métadonnées, le `sort` compactage `auto` sera automatiquement appliqué.
  - Pour les tables sans ordre de tri, le `binpack` compactage `auto` sera utilisé par défaut.
- Sac à poubelles
  - Combine de petits fichiers en fichiers plus volumineux, en ciblant généralement des tailles supérieures à 100 Mo, tout en appliquant les suppressions en attente. Il s'agit de la stratégie de compactage par défaut pour les tables non triées.
- Tri
  - Organise les données en fonction de colonnes spécifiées qui sont triées automatiquement par hiérarchie lors du compactage, améliorant ainsi les performances des requêtes pour les opérations filtrées. Cette stratégie est recommandée lorsque vos requêtes filtrent fréquemment sur des colonnes spécifiques. Lorsque vous utilisez cette stratégie, S3 Tables applique

automatiquement un tri hiérarchique aux colonnes lorsque a `sort_order` est défini dans les propriétés de la table.

- Ordre Z
  - Optimise l'organisation des données en fusionnant plusieurs attributs en une seule valeur scalaire qui peut être utilisée pour le tri, ce qui permet d'effectuer des requêtes efficaces sur plusieurs dimensions. Cette stratégie est recommandée lorsque vous devez interroger des données sur plusieurs dimensions simultanément. Cette stratégie vous oblige à définir un ordre de tri dans les propriétés de votre table Iceberg à l'aide de la propriété `sort_order` table.

Le compactage entraînera des coûts supplémentaires. Pour plus d'informations, consultez les informations de tarification dans Tarification Amazon S3.

Exemples de compactage

Les exemples suivants présentent des configurations pour le compactage des tables.

Pour configurer la taille du fichier cible de compactage à l'aide du AWS CLI

La taille minimale du fichier de compactage cible est de 64 Mo ; la taille maximale est de 512 Mo.

L'exemple suivant modifie la taille du fichier cible en la définissant sur 256 Mo à l'aide de l'API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1 \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"enabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

Pour plus d'informations, consultez put-table-maintenance-configuration dans la Référence des commandes de l'AWS CLI .

Pour configurer la stratégie de compactage à l'aide du AWS CLI

L'exemple suivant modifiera la stratégie de compactage en `sort` utilisant l'`PutTableMaintenanceConfiguration`API. Lorsque vous définissez le compactage, vous pouvez choisir l'une des stratégies de compactage suivantes :`auto`,`binpack`, ou `sort` `z-order`

> **Note**
>
> Pour définir la stratégie de compactage sur `sort` ou `z-order` vous devez remplir les conditions préalables suivantes :
>
> - Ordre de tri défini dans les propriétés de votre Iceberg table.
> - L'`s3tables:GetTableData`autorisation.

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"enabled","settings":{"icebergCompaction":
{"strategy":"sort"}}}'
```

Pour plus d'informations, consultez put-table-maintenance-configuration dans la Référence des commandes de l'AWS CLI .

Pour désactiver le compactage à l'aide du AWS CLI

L'exemple suivant permet de désactiver le compactage à l'aide de l'API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
   --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
   --type icebergCompaction \
   --namespace mynamespace \
   --name testtable \
   --value='{"status":"disabled","settings":{"icebergCompaction":
{"targetFileSizeMB":256}}}'
```

Pour plus d'informations, consultez put-table-maintenance-configuration dans la Référence des commandes de l'AWS CLI .

Gestion des instantanés

La gestion des instantanés détermine le nombre d'instantanés actifs pour votre table. Ceci est basé sur les paramètres `MinimumSnapshots` (1 par défaut) et `MaximumSnapshotAge` (120 heures par défaut). La gestion des instantanés expire et supprime les instantanés de table en fonction de ces configurations.

Lorsqu'un instantané expire, Amazon S3 marque tous les objets référencés uniquement par cet instantané comme non actuels. Ces objets non actuels sont supprimés après le nombre de jours spécifié par la propriété `NoncurrentDays` dans votre politique de suppression des fichiers non référencés.

> **Note**
>
> Les suppressions des objets non actuels sont permanentes et il n'est pas possible de récupérer ces objets.

Pour consulter ou récupérer des objets marqués comme non actuels, vous devez contacter AWS Support. Pour plus d'informations sur la prise de contact AWS Support, consultez la section Contact AWS ou la AWS Support documentation.

La gestion des instantanés détermine les objets à supprimer de votre tableau en faisant uniquement référence à ce tableau. Les références à ces objets depuis l'extérieur du tableau n'empêcheront pas la gestion des snapshots de les supprimer.

> **Note**
>
> La gestion des instantanés ne prend pas en charge les valeurs de conservation que vous configurez en tant que propriétés de table Iceberg dans le fichier `metadata.json` ou via une commande SQL `ALTER TABLE SET TBLPROPERTIES`, y compris la conservation basée sur les branches ou les balises. La gestion des instantanés est désactivée lorsque vous configurez une politique de conservation basée sur les branches ou les balises, ou lorsque vous configurez une politique de conservation sur le fichier `metadata.json` qui est plus longue que les valeurs configurées via l'API `PutTableMaintenanceConfiguration`. Dans ces cas, S3 n'expire pas et ne supprime pas les instantanés, et vous devez supprimer manuellement les instantanés ou supprimer les propriétés de votre table Iceberg pour éviter les frais de stockage.

Vous pouvez uniquement configurer la gestion des instantanés au niveau de la table. Pour plus d'informations, consultez les informations de tarification dans Tarification Amazon S3.

Exemples de gestion des snapshots

Les exemples suivants présentent des configurations pour la gestion des instantanés de table.

Pour configurer la gestion des snapshots à l'aide du AWS CLI

L'exemple suivant définit le paramètre `MinimumSnapshots` sur 10 et le paramètre `MaximumSnapshotAge` sur 2 500 heures à l'aide de l'API `PutTableMaintenanceConfiguration`.

```
aws s3tables put-table-maintenance-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
--namespace my_namespace \
--name my_table \
--type icebergSnapshotManagement \
--value '{"status":"enabled","settings":{"icebergSnapshotManagement":
{"minSnapshotsToKeep":10,"maxSnapshotAgeHours":2500}}}'
```

Pour désactiver la gestion des snapshots à l'aide du AWS CLI

L'exemple suivant désactivera la gestion des snapshots à l'aide de l'`PutTableMaintenanceConfiguration`API.

```
aws s3tables put-table-maintenance-configuration \
--table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
--namespace my_namespace \
--name my_table \
--type icebergSnapshotManagement \
--value '{"status":"disabled","settings":{"icebergSnapshotManagement":
{"minSnapshotsToKeep":1,"maxSnapshotAgeHours":120}}}'
```

Pour plus d'informations, consultez put-table-maintenance-configuration dans la Référence des commandes de l'AWS CLI .

Considérations et restrictions

Pour en savoir plus sur les considérations et les restrictions supplémentaires relatives au compactage et à la gestion des instantanés, consultez the section called "Considérations et restrictions".

> **Note**
>
> S3 Tables applique la row-group-default taille des parquets de 128 Mo.

Considérations et restrictions relatives aux tâches de maintenance

Amazon S3 propose des opérations de maintenance pour améliorer les performances de vos tables ou compartiments de tables S3. Ces options sont le compactage des fichiers, la gestion des instantanés et la suppression des fichiers non référencés. Les restrictions et considérations suivantes se rapportent à ces options de gestion.

Rubriques

- Considérations relatives au compactage
- Considérations relatives à la gestion des instantanés
- Considérations relatives à la suppression des fichiers non référencés
- Limites pour la maintenance des tables et des compartiments de tables S3

Considérations relatives au compactage

Les considérations suivantes se rapportent au compactage. Pour plus d'informations sur le compactage, consultez the section called "Maintenance des tables".

- Le compactage est pris en charge sur Apache Parquet les types de ORC fichiersAvro, et.
- Le compactage écrit les nouveaux fichiers au Apache Parquet format par défaut. Pour compacter les fichiers au ORC format Avro or à la place, définissez la propriété du `write.format.default` tableau sur `avro` ou`orc`.
- Le compactage ne prend pas en charge le type de données : fixe.
- Le compactage ne prend pas en charge les types de compression : `brotli`, `lz4`.

Considérations relatives à la gestion des instantanés

Les considérations suivantes se rapportent à la gestion des instantanés. Pour plus d'informations sur la gestion des instantanés, consultez the section called "Maintenance des tables".

- Les instantanés sont conservés seulement lorsque les deux critères suivants sont remplis : le nombre minimum d'instantanés à conserver et la période de conservation spécifiée.
- La gestion des instantanés supprime les métadonnées des instantanés expirés d'Apache Iceberg, empêchant ainsi les requêtes d'historique d'instantanés expirés et supprimant éventuellement les fichiers de données associés.
- La gestion des instantanés ne prend pas en charge les valeurs de conservation que vous configurez en tant que propriétés de table Iceberg dans le fichier `metadata.json` ou via une commande SQL `ALTER TABLE SET TBLPROPERTIES`, y compris la conservation basée sur les branches ou les balises. La gestion des instantanés est désactivée lorsque vous configurez une politique de conservation basée sur les branches ou les balises, ou lorsque vous configurez une politique de conservation sur le fichier `metadata.json` qui est plus longue que les valeurs configurées via l'API `PutTableMaintenanceConfiguration`. Dans ces cas, S3 n'expire pas et ne supprime pas les instantanés, et vous devez supprimer manuellement les instantanés ou supprimer les propriétés de votre table Iceberg pour éviter les frais de stockage.

Considérations relatives à la suppression des fichiers non référencés

Les considérations suivantes se rapportent à la suppression des fichiers non référencés. Pour plus d'informations sur la suppression des fichiers non référencés, consultez the section called "Maintenance des compartiments de tables".

- La suppression des fichiers non référencés supprime les fichiers de données et de métadonnées qui ne sont plus référencés par les métadonnées Iceberg si leur date de création est antérieure à la période de conservation.

Limites pour la maintenance des tables et des compartiments de tables S3

Opération de maintenance	Propriété	Configurable au niveau du compartiment de tables ?	Configurable au niveau de la table ?	Valeur par défaut	Valeur minimale
Compactage	targetFileSizeMB	Non	Oui	512 Mo	64 Mo
Gestion des instantanés	minimumSnapshots	Non	Oui	1	1
Gestion des instantanés	maximumSnapshotAge	Non	Oui	120 heures	1 heure
Suppression des fichiers non référencés	Jours non référencés	Oui	Non	3 jours	1 jour
Suppression des fichiers non référencés	nonCurrentDays	Oui	Non	10 jours	1 jour

> **Note**
>
> S3 Tables applique la row-group-default taille des parquets de 128 Mo.

Espaces de noms de tables

Lorsque vous créez des tables dans votre compartiment de tables Amazon S3, vous les organisez en groupes logiques appelés espaces de noms. Contrairement aux tables S3 et aux compartiments de tables, les espaces de noms ne sont pas des ressources. Les espaces de noms sont des structures qui vous aident à organiser et à gérer vos tables de manière évolutive. Par exemple, toutes les tables appartenant au service des ressources humaines d'une entreprise peuvent être regroupées sous une valeur d'espace de noms commune de`hr`.

Pour contrôler l'accès à des espaces de noms spécifiques, vous pouvez utiliser des politiques de ressources de compartiments de tables. Pour de plus amples informations, veuillez consulter the section called “Politiques basées sur les ressources”.

Les règles suivantes s'appliquent aux espaces de noms de tables :

- Chaque espace de noms doit être unique au sein d'un bucket de table.
- Vous pouvez créer jusqu'à 10 000 espaces de noms par compartiment de table.
- Chaque nom de table doit être unique au sein d'un espace de noms.
- Chaque table ne peut comporter qu'un seul niveau d'espaces de noms. Les espaces de noms ne peuvent pas être imbriqués.
- Chaque table appartient à un seul espace de noms.
- Vous pouvez déplacer vos tables entre les espaces de noms.

Rubriques

- Création d'un espace de noms
- Suppression d’un espace de noms

Création d'un espace de noms

Un espace de noms de table est une construction logique sous laquelle vous regroupez les tables au sein d'un compartiment de tables Amazon S3. Chaque table appartient à un seul espace de noms. Avant de créer une table dans un bucket de tables, vous devez créer un espace de noms dans lequel les tables seront regroupées. Vous pouvez créer un espace de noms à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 ou de moteurs de requêtes intégrés. AWS SDKs

Noms d’espace de noms

Les règles de dénomination suivantes s’appliquent aux espaces de noms :

- Les noms doivent comporter entre 1 et 255 caractères.
- Les noms ne peuvent être composés que de lettres minuscules, de chiffres et de traits de soulignement (). _ Les traits de soulignement ne sont pas autorisés au début ou à la fin des noms d'espaces de noms.
- Les noms doivent commencer et se terminer par une lettre ou un chiffre.

- Les noms ne doivent pas contenir de tirets (-) ni de points (.).
- Un espace de noms doit être unique dans un compartiment de tables.
- Les noms d'espaces de noms ne doivent pas commencer par le préfixe aws réservé.

Pour plus d'informations sur les noms d'espaces de noms valides, consultezRègles de dénomination des tables et des espaces de noms.

Utilisation de la console S3 et d'Amazon Athena

La procédure suivante utilise le flux de travail Create table with Athena pour créer un espace de noms dans la console Amazon S3. Si vous ne souhaitez pas également utiliser Amazon Athena pour créer une table dans votre espace de noms, vous pouvez annuler le flux de travail après avoir créé votre espace de noms.

Pour créer un espace de noms

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
3. Sur la page Compartiments de table, choisissez le compartiment dans lequel vous souhaitez créer un espace de noms.
4. Sur la page des détails du bucket, choisissez Create table with Athena.
5. Dans la boîte de dialogue Créer une table avec Athena, choisissez Create a namespace, puis Create namespace.
6. Entrez un nom dans le champ Nom de l'espace de noms. Les noms des espaces de noms doivent comporter de 1 à 255 caractères et être uniques dans le compartiment de table. Les caractères valides sont a—z, 0—9 et les traits de soulignement (). _ Les traits de soulignement ne sont pas autorisés au début ou à la fin des noms d'espaces de noms.
7. Choisissez Create namespace (Créer un espace de noms).
8. Si vous souhaitez également créer une table, choisissez Créer une table avec Athéna. Pour plus d'informations sur la création d'une table avec Athena, consultez. the section called “Utilisation de la console S3 et d'Amazon Athena” Si vous ne souhaitez pas créer de tableau pour le moment, choisissez Annuler.

En utilisant le AWS CLI

Cet exemple montre comment créer un espace de noms de tables à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3tables create-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
    --namespace example_namespace
```

Utilisation d'un moteur de requête

Vous pouvez créer un espace de noms dans une session Apache Spark connectée à vos compartiments de tables Amazon S3.

Cet exemple montre comment créer une table en utilisant les instructions `CREATE` dans un moteur de requête intégré avec S3 Tables. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
spark.sql("CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

Suppression d'un espace de noms

Avant de supprimer un espace de noms de table d'un compartiment de tables Amazon S3, vous devez supprimer toutes les tables de cet espace de noms ou les déplacer dans un autre espace de noms. Vous pouvez supprimer un espace de noms à l'aide de l'API REST Amazon S3 AWS SDKs, AWS Command Line Interface (AWS CLI) ou des moteurs de requête intégrés.

Pour plus d'informations sur les autorisations requises pour supprimer un espace de noms, consultez le DeleteNamespacemanuel Amazon Simple Storage Service API Reference.

En utilisant le AWS CLI

Cet exemple montre comment supprimer un espace de noms de tables à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3tables delete-namespace \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
```

```
    --namespace example_namespace
```

Tables dans des seaux de table S3

Une table S3 représente un jeu de données structuré composé de données de table sous-jacentes et des métadonnées associées. Ces données sont stockées dans un compartiment de tables en tant que sous-ressource. Toutes les tables figurant dans un compartiment de tables sont stockées au format de table Apache Iceberg. Amazon S3 gère la maintenance de vos tables via le compactage automatique des fichiers et la gestion des instantanés. Pour de plus amples informations, veuillez consulter Entretien des tables.

Pour rendre les tables de votre compte accessibles par les services AWS d'analyse, vous devez intégrer vos compartiments de tables Amazon S3 à Amazon SageMaker Lakehouse. Cette intégration permet aux services AWS d'analyse tels qu'Amazon Athena et Amazon Redshift de découvrir et d'accéder automatiquement aux données de vos tables.

Lorsque vous créez une table, Amazon S3 génère automatiquement un emplacement d'entrepôt pour cette table. Il s'agit d'un emplacement S3 unique qui stocke les objets associés à la table. L'exemple suivant illustre le format d'un emplacement d'entrepôt :

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

Au sein de votre compartiment de tables, vous pouvez organiser les tables en regroupements logiques appelés espaces de noms. Pour de plus amples informations, veuillez consulter Espaces de noms de tables.

Vous pouvez renommer des tables, mais chaque table possède son propre Amazon Resource Name (ARN) et son propre ID de table unique. Une politique de ressources est également attachée à chaque table. Vous pouvez utiliser cette politique pour gérer l'accès à la table.

Le tableau ARNs utilise le format suivant :

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

Par défaut, vous pouvez créer jusqu'à 10 000 tables dans un bucket de tables. Pour demander une augmentation de quota pour les compartiments de tables ou les tables, contactez Support.

Amazon S3 prend en charge les types de tables suivants dans les compartiments de tables :

Tables destinées aux clients

Les tables client sont des tables dans lesquelles vous pouvez lire et écrire. Vous pouvez récupérer les données de ces tables à l'aide de moteurs de requête intégrés. Vous pouvez y insérer, mettre à jour ou supprimer des données à l'aide des opérations d'API S3 ou des moteurs de requête intégrés.

AWS tables

AWS les tables sont des tables en lecture seule qui sont générées par et en votre Service AWS nom. Ces tables sont gérées par Amazon S3 et ne peuvent être modifiées par aucun principal IAM en dehors d'Amazon S3 lui-même. Vous pouvez récupérer des informations à partir de ces tables, mais vous ne pouvez pas modifier les données qu'elles contiennent. AWS les tables incluent les tables de métadonnées S3, qui contiennent des métadonnées capturées à partir des objets d'un compartiment à usage général S3. Pour de plus amples informations, veuillez consulter Accélération de la découverte des données avec les métadonnées S3.

Rubriques

- Création d'une table Amazon S3
- Suppression d'une table Amazon S3
- Gestion des politiques de tables

Création d'une table Amazon S3

Une table Amazon S3 est une sous-ressource d'un bucket de tables. Les tables sont stockées dans le Apache Iceberg format afin que vous puissiez travailler avec eux à l'aide de moteurs de requêtes et d'autres applications compatibles Apache Iceberg. Amazon S3 optimise en permanence vos tables afin de réduire les coûts de stockage et d'améliorer les performances des requêtes analytiques.

Lorsque vous créez une table, Amazon S3 génère automatiquement un emplacement d'entrepôt pour la table. Un emplacement d'entrepôt est un emplacement S3 unique dans lequel vous pouvez lire et écrire des objets associés à la table. L'exemple suivant illustre le format d'un emplacement d'entrepôt :

```
s3://63a8e430-6e0b-46f5-k833abtwr6s8tmtsycedn8s4yc3xhuse1b--table-s3
```

Les tables possèdent le format d'Amazon Resource Name (ARN) suivant :

```
arn:aws:s3tables:region:owner-account-id:bucket/bucket-name/table/table-id
```

Par défaut, vous pouvez créer jusqu'à 10 000 tables dans un bucket de tables. Pour demander une augmentation de quota pour les compartiments de tables ou les tables, contactez Support.

Vous pouvez créer une table à l'aide de la console Amazon S3, de l'API REST Amazon S3 AWS SDKs, AWS Command Line Interface (AWS CLI) ou des moteurs de requête connectés à vos compartiments de table.

Lorsque vous créez une table, vous pouvez spécifier les paramètres de chiffrement pour cette table, sauf si vous créez la table avec Athena. Si vous ne spécifiez pas de paramètres de chiffrement, la table est chiffrée avec les paramètres par défaut du compartiment de table. Pour de plus amples informations, veuillez consulter Spécification du chiffrement pour les tables.

Conditions préalables à la création de tables

Pour créer une table, vous devez d'abord effectuer les opérations suivantes :

- Créer un compartiment de tables.
- Création d'un espace de nomsdans votre seau de table.
- Assurez-vous que vous disposez des autorisations AWS Identity and Access Management (IAM) pour `s3tables:CreateTable` et`s3tables:PutTableData`.
- > **Note**
  >
  > Si vous utilisez le chiffrement SSE-KMS pour votre table, vous devez disposer d'autorisations et `s3tables:PutTableEncryption` `DescribeKey` d'autorisations pour la clé choisie AWS KMS . En outre, la AWS KMS clé que vous utilisez doit autoriser S3 Tables à effectuer la maintenance automatique des tables. Pour de plus amples informations, consultez Exigences d'autorisation pour le chiffrement SSE-KMS des tables S3.

Pour plus d'informations sur les noms de table valides, consultezRègles de dénomination des tables et des espaces de noms.

> **Important**
>
> Lorsque vous créez des tables, assurez-vous d'utiliser toutes les lettres minuscules dans les noms et les définitions de tables. Par exemple, assurez-vous que les noms de vos colonnes sont tous en minuscules. Si le nom ou la définition de votre table contient des majuscules, le tableau n'est pas pris en charge par AWS Lake Formation le AWS Glue Data Catalog. Dans ce cas, votre table ne sera pas visible par les services d' AWS analyse tels qu'Amazon Athena, même si vos compartiments de tables sont intégrés aux AWS services d'analyse. Si la définition de votre table contient des majuscules, le message d'erreur suivant s'affiche lorsque vous exécutez une `SELECT` requête dans Athena : « GENERIC_INTERNAL_ERROR : Get table request failed : com.amazonaws.services.glue.model. ValidationException: ressource de fédération non prise en charge - Noms de table ou de colonne non valides. »

Utilisation de la console S3 et d'Amazon Athena

La procédure suivante utilise la console Amazon S3 pour créer une table avec Amazon Athena. Si vous n'avez pas encore créé d'espace de noms dans votre compartiment de table, vous pouvez le faire dans le cadre de ce processus. Avant d'effectuer les étapes suivantes, assurez-vous d'avoir intégré vos compartiments de tables aux services AWS d'analyse de cette région. Pour de plus amples informations, veuillez consulter the section called “Utilisation de tables S3 avec des services AWS d'analyse”.

> **Note**
>
> Lorsque vous créez une table à l'aide d'Athena, cette table hérite des paramètres de chiffrement par défaut du compartiment de table. Si vous souhaitez utiliser un autre type de chiffrement, vous devez créer la table à l'aide d'une autre méthode.

Pour créer une table

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
3. Sur la page Compartiments de table, choisissez le compartiment dans lequel vous souhaitez créer une table.

4. Sur la page des détails du bucket, choisissez Create table with Athena.
5. Dans la boîte de dialogue Créer une table avec Athena, effectuez l'une des opérations suivantes :
   - Créez un nouvel espace de noms. Choisissez Créer un espace de noms, puis entrez un nom dans le champ Nom de l'espace de noms. Les noms des espaces de noms doivent comporter de 1 à 255 caractères et être uniques dans le compartiment de table. Les caractères valides sont a—z, 0—9 et les traits de soulignement (). _ Les traits de soulignement ne sont pas autorisés au début des noms d'espaces de noms.
   - Choisissez Create namespace (Créer un espace de noms).
   - Spécifiez un espace de noms existant. Choisissez Spécifier un espace de noms existant dans ce compartiment de table. Choisissez ensuite Choisir parmi les espaces de noms existants ou Entrez un nom d'espace de noms existant. Si votre bucket contient plus de 1 000 espaces de noms, vous devez saisir le nom de l'espace de noms s'il n'apparaît pas dans la liste.
6. Choisissez Créer une table avec Athéna.
7. La console Amazon Athena s'ouvre et l'éditeur de requêtes Athena apparaît. Le champ Catalog doit être renseigné avec s3tablescatalog/ suivi du nom de votre bucket de table, par exemple, s3tablescatalog/***amzn-s3-demo-bucket*** Le champ Base de données doit être renseigné avec l'espace de noms que vous avez créé ou sélectionné précédemment.

   > **Note**
   >
   > Si vous ne voyez pas ces valeurs dans les champs Catalogue et Base de données, assurez-vous d'avoir intégré vos compartiments de tables aux services AWS d'analyse de cette région. Pour de plus amples informations, veuillez consulter the section called "Utilisation de tables S3 avec des services AWS d'analyse".

8. L'éditeur de requêtes contient un exemple de requête que vous pouvez utiliser pour créer une table. Modifiez la requête pour spécifier le nom de la table et les colonnes que vous souhaitez attribuer à votre table.
9. Lorsque vous avez terminé de modifier la requête, choisissez Exécuter pour créer votre table.

> **Note**
>
> - Si vous recevez le message d'erreur « Autorisations insuffisantes pour exécuter la requête. Le principal n'a aucun privilège sur la ressource spécifiée. » Lorsque vous essayez d'exécuter une requête dans Athena, vous devez obtenir les autorisations Lake Formation nécessaires sur la table. Pour de plus amples informations, veuillez consulter the section called “Octroi d'une autorisation sur une table ou une base de données”.
> - Si le message d'erreur « Iceberg ne peut pas accéder à la ressource demandée » s'affiche lorsque vous essayez d'exécuter une requête dans Athena, accédez à AWS Lake Formation la console et assurez-vous que vous vous êtes accordé des autorisations sur le catalogue de compartiments de tables et la base de données (espace de noms) que vous avez créés. Ne spécifiez pas de table lorsque vous accordez ces autorisations. Pour de plus amples informations, veuillez consulter the section called “Octroi d'une autorisation sur une table ou une base de données”.
> - Si vous recevez le message d'erreur suivant lorsque vous exécutez une `SELECT` requête dans Athena, cela est dû à la présence de lettres majuscules dans le nom de votre table ou dans le nom de vos colonnes dans la définition de votre table : « GENERIC_INTERNAL_ERROR : Get table request failed : com.amazonaws.services.glue.model. ValidationException: ressource de fédération non prise en charge - Noms de table ou de colonne non valides. » Assurez-vous que les noms des tables et des colonnes sont tous en minuscules.

Si la création de votre table a réussi, le nom de votre nouvelle table apparaît dans la liste des tables d'Athena. Lorsque vous revenez à la console Amazon S3, votre nouvelle table apparaît dans la liste des tables de la page des détails du bucket correspondant à votre bucket de table après avoir actualisé la liste.

En utilisant le AWS CLI

Cet exemple montre comment créer une table avec un schéma en utilisant AWS CLI et en spécifiant les métadonnées de la table avec JSON. Pour utiliser cet exemple, remplacez le *`user input placeholders`* par vos propres informations.

```
aws s3tables create-table --cli-input-json file://mytabledefinition.json
```

Pour le `mytabledefinition.json` fichier, utilisez l'exemple de définition de table suivant. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
{
    "tableBucketARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket",
    "namespace": "your_namespace",
    "name": "example_table",
    "format": "ICEBERG",
    "metadata": {
        "iceberg": {
            "schema": {
                "fields": [
                     {"name": "id", "type": "int","required": true},
                     {"name": "name", "type": "string"},
                     {"name": "value", "type": "int"}
                ]
            }
        }
    }
}
```

Utilisation d'un moteur de requête

Vous pouvez créer une table dans un moteur de requête compatible connecté à vos compartiments de table, par exemple dans un Apache Spark session sur Amazon EMR.

L'exemple suivant montre comment créer une table avec Spark en utilisant `CREATE` des instructions, et ajoutez des données de table en utilisant `INSERT` des instructions ou en lisant les données d'un fichier existant. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
spark.sql(
" CREATE TABLE IF NOT EXISTS s3tablesbucket.example_namespace.`example_table` (
    id INT,
    name STRING,
    value INT
)
USING iceberg "
)
```

Après avoir créé la table, vous pouvez y charger des données. Choisissez l'une des méthodes suivantes :

- Ajoutez des données dans le tableau à l'aide de l'`INSERT`instruction.

```
spark.sql(
"""
    INSERT INTO s3tablesbucket.my_namespace.my_table
    VALUES
        (1, 'ABC', 100),
        (2, 'XYZ', 200)
""")
```

- Chargez un fichier de données existant.

  1. Lisez les données dans Spark :

```
val data_file_location = "Path such as S3 URI to data file"
val data_file = spark.read.parquet(data_file_location)
```

  2. Écrivez les données dans une table Iceberg :

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

Suppression d'une table Amazon S3

Vous pouvez supprimer une table à l'aide de l'API REST Amazon S3, du AWS SDK AWS CLI ou à l'aide de moteurs de requêtes intégrés.

> **Note**
>
> S3 Tables ne prend pas en charge l'opération `DROP TABLE` avec `purge=false`. Certaines versions de Spark attribuent toujours à cet indicateur la valeur false, même lors de l'exécution de commandes `DROP TABLE PURGE`. Vous pouvez réessayer `DROP TABLE` avec `purge=true` ou utiliser l'DeleteTableAPI REST S3 Tables pour supprimer une table. Lorsque vous supprimez un tableau, les objets associés à ce tableau deviennent obsolètes et leur suppression peut prendre jusqu'à un jour.

En utilisant le AWS CLI

Cet exemple montre comment supprimer une table à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3tables delete-table \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
table-bucket \
    --namespace example_namespace --name example_table
```

Utilisation d'un moteur de requête

Vous pouvez supprimer une table dans une session Apache Spark connectée à vos compartiments de tables Amazon S3.

Cet exemple montre comment supprimer une table à l'aide de la commande `DROP TABLE PURGE`. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
spark.sql(
" DROP TABLE [IF EXISTS] s3tablesbucket.example_namespace.example_table PURGE")
```

Gestion des politiques de tables

Vous pouvez ajouter, supprimer, mettre à jour et consulter les politiques relatives aux tables à l'aide de l'API REST Amazon S3, du AWS SDK et du AWS CLI. Pour plus d'informations, consultez les rubriques suivantes. Pour plus d'informations sur les actions AWS Identity and Access Management (IAM) et les clés de condition prises en charge pour les tables Amazon S3, consultezGestion des accès pour S3 Tables. Pour obtenir des exemples de politiques de tables, consultez Politiques basées sur les ressources pour S3 Tables.

Ajout d'une politique de tables

Pour ajouter une politique de table à une table, vous pouvez utiliser l'API REST Amazon S3, le AWS SDK et le AWS CLI.

À l'aide du AWS CLI

Cet exemple montre comment créer une politique de tables à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3tables put-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1 \
    --namespace my-namespace \
    --name my-table \
    --resource-policy your-policy-JSON
```

Consultation d'une politique de tables

Pour consulter la politique de compartiment attachée à un tableau, vous pouvez utiliser l'API REST Amazon S3, le AWS SDK et le AWS CLI.

À l'aide du AWS CLI

Cet exemple montre comment visualiser la politique attachée à une table à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3tables get-table-policy \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1/table/tableID \
    --namespace my-namespace \
    --name my-table
```

Suppression d'une politique de tables

Pour supprimer une politique attachée à une table, vous pouvez utiliser l'API REST Amazon S3, le AWS SDK et le AWS CLI.

À l'aide du AWS CLI

Cet exemple montre comment supprimer une politique de tables à l'aide de l' AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3tables delete-table-policy \
    --table-ARN arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket1/
table/tableID \
    --namespace your-namespace \
    --name your-table
```

Accès aux données des tables

Il existe plusieurs manières d'accéder aux tables dans les compartiments de tables Amazon S3. Vous pouvez intégrer des tables à des services d' AWS analyse à l'aide d'Amazon SageMaker Lakehouse ou accéder aux tables directement à l'aide du point de Iceberg REST terminaison Amazon S3 Tables ou du catalogue de tables Amazon S3 pour. Apache Iceberg La méthode d'accès que vous utiliserez dépendra de la configuration de votre catalogue, de votre modèle de gouvernance et de vos besoins en matière de contrôle d'accès. Vous trouverez ci-dessous un aperçu de ces méthodes d'accès.

Intégration avec Amazon SageMaker Lakehouse

Il s'agit de la méthode d'accès recommandée pour travailler avec des tables dans des compartiments de tables S3. L'intégration permet une gestion unifiée des tables, une gouvernance centralisée et un contrôle d'accès précis entre plusieurs services AWS d'analyse.

Accès direct

Utilisez cette méthode si vous devez travailler avec des implémentations de catalogues AWS Partner Network (APN), des implémentations de catalogues personnalisés ou si vous devez uniquement effectuer des read/write opérations de base sur les tables d'un seul compartiment de tables.

> **Note**
>
> Pour accéder aux tables, l'identité IAM que vous utilisez doit accéder aux ressources de vos tables et aux actions de S3 Tables. Pour de plus amples informations, veuillez consulter Gestion des accès pour S3 Tables.

Accès aux tables via l'intégration Amazon SageMaker Lakehouse

Vous pouvez intégrer des compartiments de tables S3 à Amazon SageMaker Lakehouse pour accéder aux tables à partir de services AWS d'analyse, tels qu'Amazon Athena, Amazon Redshift et. QuickSight Amazon SageMaker Lakehouse unifie vos données entre les lacs de données Amazon S3 et les entrepôts de données Amazon Redshift, afin que vous puissiez créer des applications d'analyse, d'apprentissage automatique (ML) et d'IA générative sur une seule copie des données. L'intégration remplit les ressources AWS Glue Data Catalog de votre table et fédère l'accès à ces

ressources avec. AWS Lake Formation Pour plus d'informations sur l'intégration, consultezUtilisation d'Amazon S3 Tables avec des services AWS d'analyse.

L'intégration permet un contrôle d'accès précis AWS Lake Formation afin de renforcer la sécurité. Lake Formation utilise une combinaison de son propre modèle d'autorisations et du modèle d'autorisations IAM pour contrôler l'accès aux ressources des tables et aux données sous-jacentes. Cela signifie qu'une demande d'accès à votre table doit passer les contrôles d'autorisation effectués à la fois par IAM et par Lake Formation. Pour plus d'informations, consultez la présentation des autorisations de Lake Formation dans le Guide du AWS Lake Formation développeur.

Les services AWS d'analyse suivants peuvent accéder aux tables via cette intégration :

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

Accès aux tables à l'aide du AWS GlueIceberg REST point de terminaison

Une fois que vos compartiments de tables S3 sont intégrés à Amazon SageMaker Lakehouse, vous pouvez également utiliser le AWS GlueIceberg REST point de terminaison pour vous connecter aux tables S3 à partir de moteurs de requêtes tiers compatibles. Iceberg Pour de plus amples informations, veuillez consulter Accès aux tables Amazon S3 à l'aide du AWS GlueIceberg REST point de terminaison.

Nous vous recommandons d'utiliser le AWS GlueIceberg REST point de terminaison lorsque vous souhaitez accéder à des tables à partir de Spark clients compatibles ou à partir d'autres clients Iceberg compatibles. PyIceberg

Les clients suivants peuvent accéder aux tables directement via le AWS GlueIceberg REST point de terminaison :

- N'importe quel Iceberg client, y compris SparkPyIceberg, et plus encore.

Accès direct aux tables

Vous pouvez accéder aux tables directement à partir de moteurs de requêtes open source grâce à des méthodes qui relient les opérations de gestion des tables S3 à vos applications Apache Iceberg d'analyse. Il existe deux méthodes d'accès direct : le point de Iceberg REST terminaison Amazon S3 Tables ou le catalogue de tables Amazon S3 pourApache Iceberg. Le REST point final est recommandé.

Nous recommandons un accès direct si vous accédez aux tables dans le cadre d'implémentations de catalogues autogérées ou si vous devez uniquement effectuer des read/write opérations de base sur les tables d'un seul compartiment de tables. Pour les autres scénarios d'accès, nous recommandons l'intégration Amazon SageMaker Lakehouse.

L'accès direct aux tables est géré par le biais de politiques basées sur l'identité IAM ou de politiques basées sur les ressources associées aux tables et aux compartiments de tables. Vous n'avez pas besoin de gérer les autorisations de Lake Formation pour les tables lorsque vous y accédez directement.

Accès aux tables via le point de Iceberg REST terminaison Amazon S3 Tables

Vous pouvez utiliser le point de Iceberg REST terminaison Amazon S3 Tables pour accéder à vos tables directement depuis n'importe quel client Iceberg REST compatible via des HTTP points de terminaison. Pour plus d'informations, consultezAccès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison.

Les services AWS d'analyse et moteurs de requêtes suivants peuvent accéder aux tables directement via le point de Iceberg REST terminaison Amazon S3 Tables :

Moteurs de requêtes pris en charge

- N'importe quel Iceberg client, y compris SparkPyIceberg, et plus encore.
- Amazon EMR
- AWS Glue ETL

Accès aux tables directement via le catalogue de tables Amazon S3 pour Apache Iceberg

Vous pouvez également accéder aux tables directement à partir des moteurs de requêtes, Apache Spark par exemple en utilisant le catalogue client S3 Tables. Pour plus d'informations, voirAccès aux

tables Amazon S3 avec le catalogue de tables Amazon S3 pour Apache Iceberg. S3 recommande toutefois d'utiliser le point de Iceberg REST terminaison Amazon S3 Tables pour un accès direct, car il prend en charge un plus grand nombre d'applications, sans nécessiter de langage ou de code spécifique au moteur.

Les moteurs de requête suivants peuvent accéder aux tables directement à l'aide du catalogue client :

- Apache Spark

Utilisation d'Amazon S3 Tables avec des services AWS d'analyse

Pour rendre les tables de votre compte accessibles par les services AWS d'analyse, vous devez intégrer vos compartiments de tables Amazon S3 à Amazon SageMaker Lakehouse. Cette intégration permet aux services AWS d'analyse de découvrir et d'accéder automatiquement aux données de votre table. Vous pouvez utiliser cette intégration pour utiliser vos tables dans les services suivants :

- Amazon Athena
- Amazon Redshift
- Amazon EMR
- QuickSight
- Amazon Data Firehose

> **Note**
>
> Cette intégration utilise les AWS Lake Formation services AWS Glue et peut entraîner des coûts de AWS Glue demande et de stockage. Pour plus d'informations, consultez Tarification d'AWS Glue.
> Une tarification supplémentaire s'applique à l'exécution de requêtes sur vos tables S3. Pour plus d'informations, consultez les informations tarifaires du moteur de requête que vous utilisez.

Fonctionnement de l'intégration

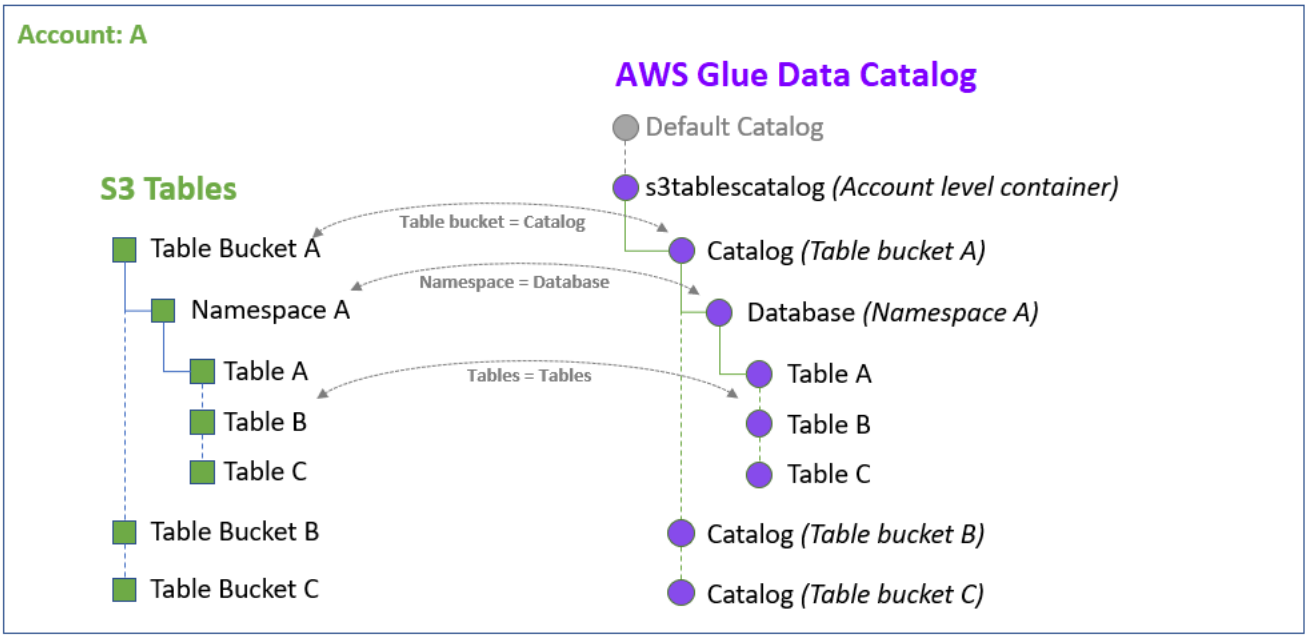
Lorsque vous créez un compartiment de table dans la console, Amazon S3 lance les actions suivantes pour intégrer les compartiments de table dans la région que vous avez sélectionnée aux services AWS d'analyse :

1. Crée un nouveau rôle de service AWS Identity and Access Management (IAM) qui permet à Lake Formation d'accéder à tous vos compartiments de table.
2. Grâce à ce rôle de service, Lake Formation enregistre des compartiments de tables dans la région actuelle. Cela permet à Lake Formation de gérer l'accès, les autorisations et la gouvernance pour tous les compartiments de tables actuels et futurs de cette région.
3. Ajoute le `s3tablescatalog` catalogue AWS Glue Data Catalog à la région actuelle. L'ajout du `s3tablescatalog` catalogue permet de renseigner tous vos compartiments de tables, espaces de noms et tables dans le catalogue de données.

> **Note**
>
> Ces actions sont automatisées via la console Amazon S3. Si vous effectuez cette intégration par programmation, vous devez effectuer toutes ces actions manuellement.

Vous intégrez vos compartiments de table une fois par AWS région. Une fois l'intégration terminée, tous les compartiments de tables, espaces de noms et tables actuels et futurs sont ajoutés AWS Glue Data Catalog dans cette région.

L'illustration suivante montre comment le `s3tablescatalog` catalogue remplit automatiquement les compartiments de tables, les espaces de noms et les tables de la région actuelle en tant qu'objets correspondants dans le catalogue de données. Les compartiments de table sont remplis sous forme de sous-catalogues. Les espaces de noms d'un bucket de tables sont renseignés sous forme de bases de données dans leurs sous-catalogues respectifs. Les tables sont renseignées en tant que tables dans leurs bases de données respectives.



Comment fonctionnent les autorisations

Nous vous recommandons d'intégrer vos compartiments de tables aux services AWS d'analyse afin de pouvoir utiliser les données de vos tables dans les services qui les utilisent AWS Glue Data Catalog comme magasin de métadonnées. L'intégration permet un contrôle d'accès précis. AWS Lake Formation Cette approche de sécurité signifie qu'en plus des autorisations AWS Identity and Access Management (IAM), vous devez accorder à votre compte principal IAM Lake Formation des autorisations sur vos tables avant de pouvoir travailler avec elles.

Il existe deux principaux types d'autorisations dans AWS Lake Formation :

- Les autorisations d'accès aux métadonnées contrôlent la capacité de créer, de lire, de mettre à jour et de supprimer des bases de données et des tables de métadonnées dans le catalogue de données.
- Les autorisations d'accès aux données sous-jacentes contrôlent la capacité à lire et à écrire des données dans les emplacements Amazon S3 sous-jacents vers lesquels pointent les ressources du catalogue de données.

Lake Formation utilise une combinaison de son propre modèle d'autorisations et du modèle d'autorisations IAM pour contrôler l'accès aux ressources du catalogue de données et aux données sous-jacentes :

- Pour qu'une demande d'accès aux ressources du catalogue de données ou aux données sous-jacentes aboutisse, elle doit passer les contrôles d'autorisation par IAM et Lake Formation.
- Les autorisations IAM contrôlent l'accès à la Formation AWS Glue APIs et aux ressources du lac, tandis que les autorisations Lake Formation contrôlent l'accès aux ressources du catalogue de données, aux sites Amazon S3 et aux données sous-jacentes.

Les autorisations de Lake Formation ne s'appliquent que dans la Région dans laquelle elles ont été accordées, et un principal doit être autorisé par un administrateur de lac de données ou un autre directeur disposant des autorisations nécessaires pour obtenir les autorisations de Lake Formation.

Pour plus d'informations, consultez Octroi d'autorisations Lake Formation du Guide du développeur AWS Lake Formation .

Assurez-vous de suivre les étapes décrites the section called "Conditions préalables à l'intégration" et the section called "Intégration de compartiments de tables aux services d' AWS analyse" de disposer des autorisations appropriées pour accéder aux ressources de AWS Glue Data Catalog votre table et pour utiliser les services d' AWS analyse.

> **Important**
>
> Si vous n'êtes pas l'utilisateur qui a effectué l'intégration des compartiments de tables aux services AWS d'analyse pour votre compte, vous devez disposer des autorisations Lake Formation nécessaires sur la table. Pour de plus amples informations, veuillez consulter the section called "Octroi d'une autorisation sur une table ou une base de données".

Conditions préalables à l'intégration

Les conditions préalables suivantes sont requises pour intégrer des compartiments de tables aux services d' AWS analyse :

- Créez un compartiment de tables.
- Associez la politique AWSLakeFormationDataAdmin AWS gérée à votre principal AWS Identity and Access Management (IAM) pour faire de cet utilisateur un administrateur de data lake. Pour plus d'informations sur la création d'un administrateur de lac de données, voir Création d'un administrateur de lac de données dans le guide du AWS Lake Formation développeur.
- Ajoutez des autorisations pour l'opération `glue:PassConnection` à votre principal IAM.

- Ajoutez des autorisations pour les `lakeformation:RegisterResourceWithPrivilegedAccess` opérations `lakeformation:RegisterResource` et à votre principal IAM.
- Effectuez une mise à jour vers la dernière version de AWS Command Line Interface (AWS CLI).

> **Important**
>
> Lorsque vous créez des tables, assurez-vous d'utiliser toutes les lettres minuscules dans les noms et les définitions de tables. Par exemple, assurez-vous que les noms de vos colonnes sont tous en minuscules. Si le nom ou la définition de votre table contient des majuscules, le tableau n'est pas pris en charge par AWS Lake Formation ou par le AWS Glue Data Catalog. Dans ce cas, votre table ne sera pas visible par les services d' AWS analyse tels qu'Amazon Athena, même si vos compartiments de tables sont intégrés aux AWS services d'analyse.
> Si la définition de votre table contient des majuscules, le message d'erreur suivant s'affiche lorsque vous exécutez une `SELECT` requête dans Athena : « GENERIC_INTERNAL_ERROR : Get table request failed : com.amazonaws.services.glue.model. ValidationException: ressource de fédération non prise en charge - Noms de table ou de colonne non valides. »

Intégration de compartiments de tables aux services d' AWS analyse

Cette intégration doit être effectuée une fois par AWS région.

> **Important**
>
> L'intégration des services d' AWS analyse utilise désormais l'`WithPrivilegedAccess`option de l'opération d'API `registerResource` Lake Formation pour enregistrer des buckets de tables S3. L'intégration crée également désormais le `s3tablescatalog` catalogue dans le AWS Glue Data Catalog en utilisant l'`AllowFullTableExternalDataAccess`option dans l'opération `CreateCatalog` AWS Glue API.
> Si vous avez configuré l'intégration avec la version préliminaire, vous pouvez continuer à utiliser votre intégration actuelle. Cependant, le processus d'intégration mis à jour permet d'améliorer les performances. Nous vous recommandons donc de procéder à la migration.

Pour migrer vers l'intégration mise à jour, consultezthe section called "Migration vers le processus d'intégration mis à jour".

Utilisation de la console S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
3. Choisissez Créer un compartiment de tables.

   La page Créer un compartiment de tables s'ouvre.
4. Entrez le nom du bucket Table et assurez-vous que la case Activer l'intégration est cochée.
5. Choisissez Créer un compartiment de tables. Amazon S3 essaiera d'intégrer automatiquement vos compartiments de tables dans cette région.

La première fois que vous intégrez des compartiments de table dans une région, Amazon S3 crée un nouveau rôle de service IAM en votre nom. Ce rôle permet à Lake Formation d'accéder à tous les compartiments de tables de votre compte et de fédérer l'accès à vos tables dans le AWS Glue Data Catalog.

À l'aide du AWS CLI

Pour intégrer des seaux de table à l'aide du AWS CLI

Les étapes suivantes montrent comment utiliser le AWS CLI pour intégrer des compartiments de table. Pour suivre ces étapes, remplacez-les *user input placeholders* par vos propres informations.

1. Créez un compartiment de tables.

```
aws s3tables create-table-bucket \
--region us-east-1 \
--name amzn-s3-demo-table-bucket
```

2. Créez un rôle de service IAM qui permet à Lake Formation d'accéder à vos ressources de table.

   a. Créez un fichier appelé `Role-Trust-Policy.json` contenant la politique de confiance suivante :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "LakeFormationDataAccessPolicy",
        "Effect": "Allow",
        "Principal": {
          "Service": "lakeformation.amazonaws.com"
        },
        "Action": [
            "sts:AssumeRole",
            "sts:SetContext",
            "sts:SetSourceIdentity"
        ],
        "Resource": "arn:aws:iam::111122223333:role/example-
lakeformation-service-role",
        "Condition": {
          "StringEquals": {
            "aws:SourceAccount": "111122223333"
          }
        }
      }
    ]
}
```

Créez le rôle de service IAM à l'aide de la commande suivante :

```
aws iam create-role \
--role-name S3TablesRoleForLakeFormation \
--assume-role-policy-document file://Role-Trust-Policy.json
```

b. Créez un fichier appelé `LF-GluePolicy.json` contenant la politique suivante :

JSON

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

```
    "Statement": [
        {
            "Sid": "LakeFormationPermissionsForS3ListTableBucket",
            "Effect": "Allow",
            "Action": [
                "s3tables:ListTableBuckets"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "LakeFormationDataAccessPermissionsForS3TableBucket",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTableBucket",
                "s3tables:GetTableBucket",
                "s3tables:CreateNamespace",
                "s3tables:GetNamespace",
                "s3tables:ListNamespaces",
                "s3tables:DeleteNamespace",
                "s3tables:DeleteTableBucket",
                "s3tables:CreateTable",
                "s3tables:DeleteTable",
                "s3tables:GetTable",
                "s3tables:ListTables",
                "s3tables:RenameTable",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:GetTableMetadataLocation",
                "s3tables:GetTableData",
                "s3tables:PutTableData"
            ],
            "Resource": [
                "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
            ]
        }
    ]
}
```

Associez la politique au rôle à l'aide de la commande suivante :

```
aws iam put-role-policy \
```

```
--role-name S3TablesRoleForLakeFormation  \
--policy-name LakeFormationDataAccessPermissionsForS3TableBucket \
--policy-document file://LF-GluePolicy.json
```

3. Créez un fichier appelé `input.json` contenant les éléments suivants :

```
{
    "ResourceArn": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",

    "WithFederation": true,
    "RoleArn": "arn:aws:iam::111122223333:role/S3TablesRoleForLakeFormation"
}
```

Enregistrez des seaux de table auprès de Lake Formation à l'aide de la commande suivante :

```
aws lakeformation register-resource \
--region us-east-1 \
--with-privileged-access \
--cli-input-json file://input.json
```

4. Créez un fichier appelé `catalog.json` contenant le catalogue suivant :

```
{
   "Name": "s3tablescatalog",
   "CatalogInput": {
      "FederatedCatalog": {
          "Identifier": "arn:aws:s3tables:us-east-1:111122223333:bucket/*",
          "ConnectionName": "aws:s3tables"
       },
       "CreateDatabaseDefaultPermissions":[],
       "CreateTableDefaultPermissions":[],
       "AllowFullTableExternalDataAccess": "True"
   }
}
```

Créez le `s3tablescatalog` catalogue à l'aide de la commande suivante. La création de ce catalogue remplit le AWS Glue Data Catalog avec des objets correspondant à des compartiments de tables, à des espaces de noms et à des tables.

```
aws glue create-catalog \
--region us-east-1 \
```

```
--cli-input-json file://catalog.json
```

5. Vérifiez que le `s3tablescatalog` catalogue a été ajouté à AWS Glue l'aide de la commande suivante :

```
aws glue get-catalog --catalog-id s3tablescatalog
```

Migration vers le processus d'intégration mis à jour

Le processus d'intégration des services d' AWS analyse a été mis à jour. Si vous avez configuré l'intégration avec la version préliminaire, vous pouvez continuer à utiliser votre intégration actuelle. Cependant, le processus d'intégration mis à jour améliore les performances. Nous vous recommandons donc de procéder à la migration en suivant les étapes suivantes. Pour plus d'informations sur le processus de migration ou d'intégration, consultez la section Création d'un catalogue de tables Amazon S3 AWS Glue Data Catalog dans le manuel du AWS Lake Formation développeur.

1. Ouvrez la AWS Lake Formation console sur https://console.aws.amazon.com/lakeformation/ et connectez-vous en tant qu'administrateur du lac de données. Pour plus d'informations sur la création d'un administrateur de lac de données, voir Création d'un administrateur de lac de données dans le guide du AWS Lake Formation développeur.
2. Supprimez votre `s3tablescatalog` catalogue en procédant comme suit :
   - Dans le volet de navigation de gauche, sélectionnez Catalogues.
   - Sélectionnez le bouton d'option situé à côté du `s3tablescatalog` catalogue dans la liste des catalogues. Dans le menu Actions, sélectionnez Delete (Supprimer).
3. Désenregistrez l'emplacement des données du `s3tablescatalog` catalogue en procédant comme suit :
   - Dans le volet de navigation de gauche, accédez à la section Administration, puis choisissez Data lake locations.
   - Sélectionnez le bouton d'option à côté de l'emplacement du lac de `s3tablescatalog` données, par exemple,`s3://tables:region:account-id:bucket/*`.
   - Dans le menu Actions, choisissez Supprimer.
   - Dans la boîte de dialogue de confirmation qui apparaît, choisissez Supprimer.

4. Maintenant que vous avez supprimé l'emplacement de votre `s3tablescatalog` catalogue et de votre lac de données, vous pouvez suivre les étapes pour intégrer vos compartiments de tables aux services AWS d'analyse en utilisant le processus d'intégration mis à jour.

> **Note**
>
> Si vous souhaitez utiliser des tables chiffrées SSE-KMS dans des services AWS d'analyse intégrés, le rôle que vous utilisez doit être autorisé à utiliser votre AWS KMS clé pour les opérations de chiffrement. Pour de plus amples informations, veuillez consulter Octroi aux principaux IAM des autorisations leur permettant de travailler avec des tables chiffrées dans les services d'analyse intégrés AWS.

Étapes suivantes

- Création d'un espace de noms.
- Créer une table .

Accorder des autorisations à Lake Formation sur les ressources de votre table

Une fois vos compartiments de tables intégrés aux services AWS d'analyse, Lake Formation gère l'accès aux ressources de vos tables. Lake Formation utilise son propre modèle d'autorisations (autorisations Lake Formation) qui permet un contrôle d'accès précis pour les ressources du catalogue de données. Lake Formation exige que chaque principal IAM (utilisateur ou rôle) soit autorisé à effectuer des actions sur les ressources gérées par Lake Formation. Pour plus d'informations, consultez Octroi d'autorisations Lake Formation du Guide du développeur AWS Lake Formation . Pour plus d'informations sur le partage de données entre comptes, voir Partage de données entre comptes dans Lake Formation dans le Guide du AWS Lake Formation développeur.

Avant que les responsables d'IAM puissent accéder aux tables des services AWS d'analyse, vous devez leur accorder des autorisations Lake Formation sur ces ressources.

> **Note**
>
> Si vous êtes l'utilisateur qui a effectué l'intégration du bucket de tables, vous disposez déjà des autorisations Lake Formation pour accéder à vos tables. Si vous êtes le seul directeur à accéder à vos tables, vous pouvez ignorer cette étape. Il vous suffit d'accorder

des autorisations Lake Formation sur vos tables aux autres principaux IAM. Cela permet aux autres principaux d'accéder à la table lors de l'exécution de requêtes. Pour de plus amples informations, veuillez consulter Octroi d'une autorisation sur une table ou une base de données.

Vous devez accorder aux autres responsables IAM des autorisations Lake Formation sur les ressources de votre table pour travailler avec eux dans les services suivants :

- Amazon Redshift
- Amazon Data Firehose
- Amazon QuickSight
- Amazon Athena

Octroi d'une autorisation sur une table ou une base de données

Vous pouvez accorder à une Lake Formation principale des autorisations sur une table ou une base de données dans un bucket de tables, soit par le biais de la console Lake Formation, soit du AWS CLI.

Note

Lorsque vous accordez des autorisations sur une ressource du catalogue de données à un compte externe ou directement à un responsable IAM d'un autre compte, Lake Formation utilise le service AWS Resource Access Manager (AWS RAM) pour partager la ressource. Si le compte du bénéficiaire appartient à la même organisation que le compte du donateur, la ressource partagée est immédiatement accessible au bénéficiaire. Si le compte du bénéficiaire n'appartient pas à la même organisation, AWS RAM envoie une invitation au compte du bénéficiaire pour qu'il accepte ou rejette la subvention de ressources. Ensuite, pour rendre la ressource partagée disponible, l'administrateur du lac de données du compte bénéficiaire doit utiliser la AWS RAM console ou AWS CLI accepter l'invitation. Pour plus d'informations sur le partage de données entre comptes, voir Partage de données entre comptes dans Lake Formation dans le guide du AWS Lake Formation développeur.

Console

1. Ouvrez la AWS Lake Formation console sur https://console.aws.amazon.com/lakeformation/ et connectez-vous en tant qu'administrateur du lac de données. Pour plus d'informations sur la création d'un administrateur de lac de données, voir Création d'un administrateur de lac de données dans le guide du AWS Lake Formation développeur.
2. Dans le volet de navigation, choisissez Autorisations relatives aux données, puis choisissez Grant.
3. Sur la page Accorder des autorisations, sous Principaux, effectuez l'une des opérations suivantes :
   - Pour Amazon Athena ou Amazon Redshift, choisissez les utilisateurs et les rôles IAM, puis sélectionnez le principal IAM que vous utilisez pour les requêtes.
   - Pour Amazon Data Firehose, choisissez les utilisateurs et les rôles IAM, puis sélectionnez le rôle de service que vous avez créé pour le streaming vers les tables.
   - Pour QuickSight, choisissez des utilisateurs et des groupes SAML, puis entrez le nom de ressource Amazon (ARN) de votre utilisateur QuickSight administrateur.
4. Sous Balises LF ou ressources de catalogue, choisissez Ressources de catalogue de données nommées.
5. Pour les catalogues, choisissez le sous-catalogue que vous avez créé lorsque vous avez intégré votre compartiment de table, par exemple,. *account-id*:s3tablescatalog/*amzn-s3-demo-bucket*
6. Pour Bases de données, choisissez l'espace de noms de compartiments de tables S3 que vous avez créé.
7. (Facultatif) Pour Tables, choisissez la table S3 que vous avez créée dans votre compartiment de tables.

   > **Note**
   >
   > Si vous créez une nouvelle table dans l'éditeur de requêtes Athena, ne sélectionnez pas de table.

8. Effectuez l'une des actions suivantes :
   - Si vous avez spécifié une table à l'étape précédente, choisissez Super pour les autorisations de table.

- Si vous n'avez pas spécifié de table à l'étape précédente, accédez à Autorisations de base de données. Pour le partage de données entre comptes, vous ne pouvez pas choisir Super pour accorder à l'autre principal toutes les autorisations sur votre base de données. Choisissez plutôt des autorisations plus détaillées, telles que Describe.

9. Choisissez Accorder.

CLI

1. Assurez-vous d'exécuter les AWS CLI commandes suivantes en tant qu'administrateur du lac de données. Pour plus d'informations, consultez la section Création d'un administrateur de lac de données dans le guide du AWS Lake Formation développeur.
2. Exécutez la commande suivante pour accorder des autorisations Lake Formation sur la table du compartiment de tables S3 à un principal IAM pour lui permettre d'accéder à la table. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws lakeformation grant-permissions \
--region us-east-1 \
--cli-input-json \
'{
    "Principal": {
        "DataLakePrincipalIdentifier": "user or role ARN, for example,
 arn:aws:iam::account-id:role/example-role"
    },
    "Resource": {
        "Table": {
            "CatalogId": "account-id:s3tablescatalog/amzn-s3-demo-bucket",
            "DatabaseName": "S3 table bucket namespace, for example,
 test_namespace",
            "Name": "S3 table bucket table name, for example test_table"
        }
    },
    "Permissions": [
        "ALL"
    ]
}'
```

Accès aux tables Amazon S3 à l'aide du AWS GlueIceberg REST point de terminaison

Une fois que vos compartiments de tables S3 sont intégrés au, AWS Glue Data Catalog vous pouvez utiliser le AWS GlueIceberg REST point de terminaison pour vous connecter à vos tables S3 à partir de clients Apache Iceberg compatibles, tels que PyIceberg ou. Spark Le AWS Glue Iceberg REST point de terminaison implémente la spécification Iceberg REST Catalog Open API qui fournit une interface standardisée pour interagir avec Iceberg les tables. Pour accéder aux tables S3 à l'aide du point de terminaison, vous devez configurer les autorisations via une combinaison de politiques et d' AWS Lake Formation autorisations IAM. Les sections suivantes expliquent comment configurer l'accès, notamment en créant le rôle IAM nécessaire, en définissant les politiques requises et en établissant les autorisations de Lake Formation pour l'accès à la base de données et au niveau de la table.

Pour une description détaillée de l'utilisation de bout en boutPyIceberg, consultez la section Accès aux données dans les tables Amazon S3 PyIceberg via le AWS GlueIceberg REST point de terminaison.

Prérequis

- Intégrez vos compartiments de table aux services d' AWS analyse
- Création d'un espace de noms de table
- Avoir accès à un compte d'administrateur de data lake

Créez un rôle IAM pour votre client

Pour accéder aux tables via des AWS Glue points de terminaison, vous devez créer un rôle IAM avec des autorisations AWS Glue et des actions sur Lake Formation. Cette procédure explique comment créer ce rôle et configurer ses autorisations.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, choisissez Politiques.
3. Choisissez Créer une politique, puis JSON dans l'éditeur de politique.
4. Ajoutez la politique en ligne suivante qui accorde des autorisations d'accès AWS Glue et des actions relatives à Lake Formation :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "glue:GetCatalog",
                "glue:GetDatabase",
                "glue:GetDatabases",
                "glue:GetTable",
                "glue:GetTables",
                "glue:CreateTable",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:aws-region:111122223333:catalog",
                "arn:aws:glue:aws-region:111122223333:catalog/
s3tablescatalog",
                "arn:aws:glue:aws-region:111122223333:catalog/
s3tablescatalog/amzn-s3-demo-table-bucket",
                "arn:aws:glue:aws-region:111122223333:table/s3tablescatalog/
amzn-s3-demo-table-bucket/<namespace>/*",
                "arn:aws:glue:aws-region:111122223333:database/
s3tablescatalog/amzn-s3-demo-table-bucket/<namespace>"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Après avoir créé la politique, créez un rôle IAM et choisissez Politique de confiance personnalisée comme type d'entité fiable.

6. Entrez ce qui suit pour la politique de confiance personnalisée.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/<Admin_role>"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

Définir l'accès dans Lake Formation

Lake Formation fournit un contrôle d'accès précis pour vos tables de lacs de données. Lorsque vous avez intégré votre compartiment S3 au AWS Glue Data Catalog, vos tables ont été automatiquement enregistrées en tant que ressources dans Lake Formation. Pour accéder à ces tables, vous devez accorder des autorisations spécifiques à Lake Formation pour votre identité IAM, en plus de ses autorisations de politique IAM.

Les étapes suivantes expliquent comment appliquer les contrôles d'accès à Lake Formation pour permettre à votre Iceberg client de se connecter à vos tables. Vous devez vous connecter en tant qu'administrateur du lac de données pour appliquer ces autorisations.

Autoriser les moteurs externes à accéder aux données des tables

Dans Lake Formation, vous devez activer l'accès complet aux tables pour que les moteurs externes puissent accéder aux données. Cela permet aux applications tierces d'obtenir des informations d'identification temporaires auprès de Lake Formation lorsqu'elles utilisent un rôle IAM disposant d'autorisations complètes sur la table demandée.

Ouvrez la console Lake Formation à l'adresse https://console.aws.amazon.com/lakeformation/.

1. Ouvrez la console Lake Formation à l'https://console.aws.amazon.com/lakeformation/adresse et connectez-vous en tant qu'administrateur de lac de données.
2. Dans le volet de navigation, sous Administration, sélectionnez Paramètres d'intégration des applications.
3. Sélectionnez Autoriser les moteurs externes à accéder aux données des emplacements Amazon S3 avec un accès complet aux tables. Ensuite, choisissez Save (Enregistrer).

Octroi des autorisations Lake Formation sur vos ressources de table

Ensuite, accordez à Lake Formation des autorisations pour le rôle IAM que vous avez créé pour votre client compatible avec Iceberg. Ces autorisations permettront au rôle de créer et de gérer des tables dans votre espace de noms. Vous devez fournir des autorisations au niveau de la base de données et au niveau de la table :

Pour accorder des autorisations de base de données

1. Ouvrez la AWS Lake Formation console sur https://console.aws.amazon.com/lakeformation/et connectez-vous en tant qu'administrateur du lac de données.
2. Dans le volet de navigation, choisissez Autorisations de données, puis Accorder.
3. Sur la page Accorder des autorisations, sous Principaux, sélectionnez Utilisateurs et rôles IAM, puis sélectionnez le rôle IAM que vous avez créé pour AWS Glue l'accès à Iceberg. REST endpoint
4. Sous Balises LF ou ressources de catalogue, choisissez Ressources de catalogue de données nommées.
5. Pour Catalogues, choisissez le catalogue de AWS Glue données créé pour votre compartiment de tables. Par exemple, *<accoundID>*`:s3tablescatalog/`*<table-bucket-name>*.
6. Pour Bases de données, sélectionnez`mynamespace`.
7. Pour les autorisations relatives aux tables, choisissez Créer une table et Décrire.
8. Choisissez Accorder.

Pour accorder des autorisations aux tables

1. Ouvrez la AWS Lake Formation console sur https://console.aws.amazon.com/lakeformation/ et connectez-vous en tant qu'administrateur du lac de données.
2. Dans le volet de navigation, choisissez Autorisations de données, puis Accorder.

3. Sur la page Accorder des autorisations, sous Principaux, sélectionnez Utilisateurs et rôles IAM, puis sélectionnez le rôle IAM que vous avez créé pour AWS Glue l'accès à Iceberg. REST endpoint
4. Sous Balises LF ou ressources de catalogue, choisissez Ressources de catalogue de données nommées.
5. Pour Catalogues, choisissez le catalogue de AWS Glue données créé pour votre compartiment de tables. Par exemple, *<accoundID>*:s3tablescatalog/*<table-bucket-name>*.
6. Pour Bases de données, choisissez l'espace de noms de compartiments de tables S3 que vous avez créé.
7. Pour Tables, choisissez ALL_TABLES.
8. Pour Autorisations de table, choisissez Super.
9. Choisissez Accorder.

Configurez votre environnement pour utiliser le point de terminaison

Après avoir configuré le rôle IAM avec les autorisations requises pour accéder aux tables, vous pouvez l'utiliser pour exécuter des Iceberg clients depuis votre machine locale en le configurant AWS CLI avec votre rôle, à l'aide de la commande suivante :

```
aws sts assume-role --role-arn "arn:aws:iam::<accountid>:role/<glue-irc-role>" --role-
session-name <glue-irc-role>
```

Pour accéder aux tables via le AWS Glue REST point de terminaison, vous devez initialiser un catalogue dans votre client Iceberg compatible. Cette initialisation nécessite de spécifier des propriétés personnalisées, notamment les propriétés sigv4, l'URI du point de terminaison et l'emplacement de l'entrepôt. Spécifiez ces propriétés comme suit :

- Propriétés Sigv4 - Sigv4 doit être activé, le nom de signature est `glue`
- Emplacement de l'entrepôt - Il s'agit de votre compartiment de table, spécifié dans ce format : *<accountid>*:s3tablescatalog/*<table-bucket-name>*
- URI du point de terminaison : reportez-vous au guide de référence des points AWS Glue de terminaison de service pour le point de terminaison spécifique à la région

L'exemple suivant montre comment initialiser un pyIceberg catalogue.

```
rest_catalog = load_catalog(
        s3tablescatalog,
**{
"type": "rest",
"warehouse": "<accountid>:s3tablescatalog/<table-bucket-name>",
"uri": "https://glue.<region>.amazonaws.com/iceberg",
"rest.sigv4-enabled": "true",
"rest.signing-name": "glue",
"rest.signing-region": region
        }
)
```

Pour plus d'informations sur l'implémentation du AWS GlueIceberg REST point de terminaison, consultez la section Connexion au catalogue de données à l'aide d'un point de AWS GlueIceberg REST terminaison dans le guide de AWS Glue l'utilisateur.

Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison

Vous pouvez connecter votre Iceberg REST client pour les tables Amazon S3 Iceberg REST endpoint et marque REST API appels pour créer, mettre à jour ou interroger des tables dans des compartiments de tables S3. Le point de terminaison implémente un ensemble de normes Iceberg REST APIs spécifiée dans le Apache Iceberg REST Spécification de l'API Catalog Open. Le point de terminaison fonctionne en traduisant Iceberg REST API opérations dans les opérations correspondantes des tables S3.

> **Note**
>
> Tables Amazon S3 Iceberg REST le point de terminaison peut être utilisé pour accéder aux tables dans les implémentations de catalogue AWS Partner Network (APN) ou les implémentations de catalogue personnalisées. Il peut également être utilisé si vous n'avez besoin que d'un accès de base en lecture/écriture à un seul compartiment de table. Pour les autres scénarios d'accès, nous vous recommandons d'utiliser le AWS Glue Iceberg REST point de terminaison pour se connecter aux tables, qui fournit une gestion unifiée des tables, une gouvernance centralisée et un contrôle d'accès précis. Pour plus d'informations, consultez Accès aux tables Amazon S3 à l'aide du AWS GlueIceberg REST point de terminaison.

Configuration du point de terminaison

Vous vous connectez aux tables Amazon S3 Iceberg REST point de terminaison utilisant le point de terminaison de service. S3 Tables Iceberg REST les points de terminaison ont le format suivant :

```
https://s3tables.<REGION>.amazonaws.com/iceberg
```

Reportez-vous à Tables Régions AWS et points de terminaison S3 pour les points de terminaison spécifiques à la région.

Propriétés de configuration du catalogue

Lorsque vous utilisez un client Iceberg pour connecter un moteur d'analyse au point de terminaison du service, vous devez spécifier les propriétés de configuration suivantes lors de l'initialisation du catalogue. Remplacez le *`placeholder values`* par les informations relatives à votre région et à votre compartiment de tables.

- Le point de terminaison spécifique à la région en tant qu'URI du point de terminaison : `https://s3tables.<REGION>.amazonaws.com/iceberg`
- L'ARN de votre compartiment de table comme emplacement de l'entrepôt : `arn:aws:s3tables:<region>:<accountID>:bucket/<bucketname>`
- Propriétés Sigv4 pour l'authentification. Le nom de signature SigV4 pour les demandes de point de terminaison de service est le suivant : `s3tables`

Les exemples suivants vous montrent comment configurer différents clients pour utiliser les tables Amazon S3 Iceberg REST point final.

PyIceberg

Pour utiliser les tables Amazon S3 Iceberg REST point de terminaison avec PyIceberg, spécifiez les propriétés de configuration de l'application suivantes :

```
rest_catalog = load_catalog(
  catalog_name,
  **{
    "type": "rest",
    "warehouse":"arn:aws:s3tables:<Region>:<accountID>:bucket/<bucketname>",
    "uri": "https://s3tables.<Region>.amazonaws.com/iceberg",
```

```
    "rest.sigv4-enabled": "true",
    "rest.signing-name": "s3tables",
    "rest.signing-region": "<Region>"
  }
)
```

Apache Spark

Pour utiliser les tables Amazon S3 Iceberg REST point de terminaison avec Spark, spécifiez les propriétés de configuration de l'application suivantes, en les *placeholder values* remplaçant par les informations relatives à votre région et à votre compartiment de table.

```
spark-shell \
  --packages "org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.4.1,software.amazon.awssdk:bundle:2.20.160,software.amazon.awssdk:url-
connection-client:2.20.160" \
  --master "local[*]" \
  --conf
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions"
 \
  --conf "spark.sql.defaultCatalog=spark_catalog" \
   --conf "spark.sql.catalog.spark_catalog=org.apache.iceberg.spark.SparkCatalog" \
  --conf "spark.sql.catalog.spark_catalog.type=rest" \
  --conf "spark.sql.catalog.spark_catalog.uri=https://
s3tables.<Region>.amazonaws.com/iceberg" \
  --conf
 "spark.sql.catalog.spark_catalog.warehouse=arn:aws:s3tables:<Region>:<accountID>:bucket/
<bucketname>" \
  --conf "spark.sql.catalog.spark_catalog.rest.sigv4-enabled=true" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-name=s3tables" \
  --conf "spark.sql.catalog.spark_catalog.rest.signing-region=<Region>" \
  --conf "spark.sql.catalog.spark_catalog.io-
impl=org.apache.iceberg.aws.s3.S3FileIO" \
  --conf
 "spark.hadoop.fs.s3a.aws.credentials.provider=org.apache.hadoop.fs.s3a.SimpleAWSCredentialP
 \
  --conf "spark.sql.catalog.spark_catalog.rest-metrics-reporting-enabled=false"
```

Authentification et autorisation d'accès au terminal

Les demandes d'API adressées aux points de terminaison du service S3 Tables sont authentifiées à l'aide de AWS Signature Version 4 (SigV4). Consultez AWS la version 4 de Signature pour les demandes d'API afin d'en savoir plus sur AWS SigV4.

Le nom de signature SigV4 pour les tables Amazon S3 Iceberg REST les demandes de point de terminaison sont : `s3tables`

Demandes adressées aux tables Amazon S3 Iceberg REST les terminaux sont autorisés à l'aide d'actions `s3tables` IAM correspondant au REST Opérations d'API. Ces autorisations peuvent être définies soit dans des politiques basées sur l'identité IAM, soit dans des politiques basées sur les ressources associées aux tables et aux compartiments de tables. Pour de plus amples informations, veuillez consulter Gestion des accès pour S3 Tables.

Vous pouvez suivre les demandes adressées à vos tables par le biais du REST point de terminaison avec AWS CloudTrail. Les demandes seront enregistrées en tant qu'action S3 IAM correspondante. Par exemple, une `LoadTable` API générera un événement de gestion pour l'`GetTableMetadataLocation`opération et un événement de données pour l'`GetTableData`opération. Pour de plus amples informations, veuillez consulter Journalisation avec AWS CloudTrail pour les tables S3.

Paramètres du préfixe et du chemin

Iceberg REST APIs les catalogues ont un préfixe de forme libre dans leur demande. URLs Par exemple, l'appel `ListNamespaces` d'API utilise le format `GET/v1/{prefix}/namespaces` URL. Pour les tables S3, le chemin `{prefix}` REST est toujours l'ARN de votre bucket de table codé en URL.

Par exemple, pour l'ARN du bucket de table suivant : `arn:aws:s3tables:`*`us-east-1`*`:111122223333:bucket/`*`bucketname`* le préfixe serait : `arn%3Aaws%3As3tables%3A`*`us-east-1`*`%3A`*`111122223333`*`%3Abucket%2F`*`bucketname`*

Paramètre de chemin d'espace de noms

Espaces de noms dans un Iceberg REST le chemin de l'API du catalogue peut comporter plusieurs niveaux. Toutefois, S3 Tables ne prend en charge que les espaces de noms à un seul niveau. Pour accéder à un espace de noms dans une hiérarchie de catalogue à plusieurs niveaux, vous pouvez vous connecter à un catalogue à plusieurs niveaux situé au-dessus de l'espace de noms lorsque vous le référencez. Cela permet à tout moteur de requête prenant en charge la notation en 3 parties

d'accéder `catalog.namespace.table` aux objets de la hiérarchie du catalogue de S3 Tables sans problèmes de compatibilité par rapport à l'utilisation de l'espace de noms à plusieurs niveaux.

Pris en charge Iceberg REST Opérations d'API

Le tableau suivant présente les REST Iceberg pris en charge APIs et indique comment ils correspondent aux actions S3 Tables.

Opération Iceberg REST	chemin REST	Action IAM des tables S3	CloudTrail EventName
`getConfig`	`GET /v1/config`	`s3tables:GetTableBucket`	`s3tables:GetTableBucket`
`listNamespaces`	`GET /v1/{prefix}/namespaces`	`s3tables:ListNamespaces`	`s3tables:ListNamespaces`
`createNamespace`	`POST /v1/{prefix}/namespaces`	`s3tables:CreateNamespace`	`s3tables:CreateNamespace`
`loadNamespaceMetadata`	`GET /v1/{prefix}/namespaces/{namespace}`	`s3tables:GetNamespace`	`s3tables:GetNamespace`
`dropNamespace`	`DELETE /v1/{prefix}/namespaces/{namespace}`	`s3tables:DeleteNamespace`	`s3tables:DeleteNamespace`
`listTables`	`GET /v1/{prefix}/namespaces/{namespace}/tables`	`s3tables:ListTables`	`s3tables:ListTables`
`createTable`	`POST /v1/{prefix}/names`	`s3tables:CreateTab`	`s3tables:CreateTab`

Opération Iceberg REST	chemin REST	Action IAM des tables S3	CloudTrail EventName
	paces/{na mespace}/ tables	le , s3tables: PutTableData	le , s3tables: PutObject
loadTable	GET /v1/{pref ix}/names paces/{na mespace}/ tables/{table}	s3tables: GetTableM etadataLo cation , s3tables: GetTableData	s3tables: GetTableM etadataLo cation , s3tables: GetObject
updateTable	POST /v1/{pref ix}/names paces/{na mespace}/ tables/{table}	s3tables: UpdateTab leMetadat aLocation , s3tables: PutTableD ata , s3tables: GetTableData	s3tables: UpdateTab leMetadat aLocation , s3tables: PutObject , s3tables: GetObject
dropTable	DELETE /v1/ {prefix}/ namespaces/ {namespace}/ tables/{table}	s3tables: DeleteTable	s3tables: DeleteTable
renameTable	POST /v1/{pref ix}/tables/ rename	s3tables: RenameTable	s3tables: RenameTable
tableExists	HEAD /v1/{pref ix}/names paces/{na mespace}/ tables/{table}	s3tables: GetTable	s3tables: GetTable

Opération Iceberg REST	chemin REST	Action IAM des tables S3	CloudTrail EventName
`namespaceExists`	`HEAD /v1/{prefix}/namespaces/{namespace}`	`s3tables:GetNamespace`	`s3tables:GetNamespace`

Considérations et restrictions

Voici les considérations et les limites relatives à l'utilisation des tables Amazon S3 : Iceberg REST point final.

Considérations

- CreateTable Comportement de l'API — L'`stage-create`option n'est pas prise en charge pour cette opération et entraîne une `400 Bad Request` erreur. Cela signifie que vous ne pouvez pas créer de table à partir des résultats d'une requête à l'aide de `CREATE TABLE AS SELECT` (CTAS).
- DeleteTable Comportement de l'API : vous ne pouvez supprimer des tables que lorsque la purge est activée. La suppression de tables avec n'`purge=false`est pas prise en charge et entraîne une `400 Bad Request` erreur. Certaines versions de Spark définissez toujours cet indicateur sur false même lors de l'exécution de `DROP TABLE PURGE` commandes. Vous pouvez essayer `DROP TABLE PURGE` ou utiliser l'DeleteTableopération S3 Tables pour supprimer une table.
- Le point de terminaison prend uniquement en charge les opérations de métadonnées de table standard. Pour la maintenance des tables, telle que la gestion des instantanés et le compactage, utilisez les opérations de l'API de maintenance des tables S3. Pour de plus amples informations, veuillez consulter Maintenance de S3 Tables.

Limites

- Les espaces de noms multiniveaux ne sont pas pris en charge.
- OAuthl'authentification basée n'est pas prise en charge.
- Seule la `owner` propriété est prise en charge pour les espaces de noms.
- Lié à la vue APIs défini dans le Apache Iceberg RESTLes spécifications d'API ouvertes ne sont pas prises en charge.

- L'exécution d'opérations sur une table contenant un `metadata.json` fichier de plus de 5 Mo n'est pas prise en charge et renverra une `400 Bad Request` erreur. Pour contrôler la taille de vos `metadata.json` fichiers, utilisez les opérations de maintenance des tables. Pour de plus amples informations, veuillez consulter Maintenance de S3 Tables.

Accès aux tables Amazon S3 avec le catalogue de tables Amazon S3 pour Apache Iceberg

Vous pouvez accéder aux tables S3 à partir de moteurs de requêtes open source tels que Apache Spark en utilisant le catalogue de tables Amazon S3 pour Apache Iceberg catalogue client. Catalogue de tables Amazon S3 pour Apache Iceberg est une bibliothèque open source hébergée par AWS Labs. Cela fonctionne en traduisant Apache Iceberg opérations dans vos moteurs de requêtes (telles que la découverte de tables, les mises à jour de métadonnées et l'ajout ou la suppression de tables) dans les opérations de l'API S3 Tables.

Catalogue de tables Amazon S3 pour Apache Iceberg est distribué sous forme de Maven JAR appelés`3-tables-catalog-for-iceberg.jar`. Vous pouvez créer le catalogue client JAR à partir du AWS Labs GitHub dépôt ou téléchargez-le depuis Maven. Lors de la connexion à des tables, le catalogue client JAR est utilisé comme dépendance lorsque vous initialisez un Spark séance pour Apache Iceberg.

Utilisation du catalogue de tables Amazon S3 pour Apache Iceberg avec Apache Spark

Vous pouvez utiliser le catalogue de tables Amazon S3 pour Apache Iceberg catalogue client pour se connecter à des tables à partir d'applications open source lorsque vous initialisez un Spark séance. Dans la configuration de votre session, vous spécifiez Iceberg et les dépendances d'Amazon S3, et créez un catalogue personnalisé qui utilise votre compartiment de tables comme entrepôt de métadonnées.

Prérequis

- Une identité IAM avec accès à votre compartiment de tables et aux actions S3 Tables. Pour de plus amples informations, veuillez consulter Gestion des accès pour S3 Tables.

Pour initialiser un Spark session utilisant le catalogue de tables Amazon S3 pour Apache Iceberg

- Initialiser Spark à l'aide de la commande suivante. Pour utiliser la commande, remplacez le catalogue de tables Amazon S3 par Apache Iceberg *version number*avec la dernière version de AWS Labs GitHub référentiel, et le *table bucket ARN* avec votre propre ARN de bucket de table.

```
spark-shell \
--packages org.apache.iceberg:iceberg-spark-
runtime-3.5_2.12:1.6.1,software.amazon.s3tables:s3-tables-catalog-for-iceberg-
runtime:0.1.4 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-table-bucket \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

Interrogation de tables S3 avec Spark SQL

Utilisation Spark, vous pouvez exécuter des opérations DQL, DML et DDL sur des tables S3. Lorsque vous interrogez des tables, vous utilisez le nom complet de la table, y compris le nom du catalogue de sessions, selon le modèle suivant :

CatalogName.*NamespaceName*.*TableName*

Les exemples de requêtes suivants montrent plusieurs manières d'interagir avec les tables S3. Pour utiliser ces exemples de requêtes dans votre moteur de requêtes, remplacez les *user input placeholder* valeurs par les vôtres.

Pour interroger des tables avec Spark

- Création d'un espace de noms

```
spark.sql(" CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.my_namespace")
```

- Créer une table

```
spark.sql(" CREATE TABLE IF NOT EXISTS s3tablesbucket.my_namespace.`my_table`
```

```
( id INT, name STRING, value INT ) USING iceberg ")
```

- Interroger une table

```
spark.sql(" SELECT * FROM s3tablesbucket.my_namespace.`my_table` ").show()
```

- Insérer des données dans un tableau

```
spark.sql(
"""
    INSERT INTO s3tablesbucket.my_namespace.my_table
    VALUES
        (1, 'ABC', 100),
        (2, 'XYZ', 200)
""")
```

- Charger un fichier de données existant dans une table

1. Lisez les données dans Spark.

```
val data_file_location = "Path such as S3 URI to data file"
val data_file = spark.read.parquet(data_file_location)
```

2. Écrivez les données dans une table Iceberg.

```
data_file.writeTo("s3tablesbucket.my_namespace.my_table").using("Iceberg").tableProperty
 ("format-version", "2").createOrReplace()
```

Interrogation des tables Amazon S3 avec Athena

Amazon Athena est un service de requête interactif que vous pouvez utiliser pour analyser des données directement dans Amazon S3 à l'aide du SQL standard. Pour de plus amples informations, veuillez consulter Qu'est-ce que Amazon Athena ? dans le Guide de l'utilisateur d'Amazon Athena.

Après avoir intégré vos compartiments de tables aux services AWS d'analyse, vous pouvez exécuter des requêtes en langage de définition de données (DDL), en langage de manipulation de données (DML) et en langage de requête de données (DQL) sur des tables S3 à l'aide d'Athena. Pour plus d'informations sur la manière d'interroger des tables dans un compartiment de tables, consultez la section Enregistrer les catalogues de compartiments de tables S3 dans le guide de l'utilisateur d'Amazon Athena.

Vous pouvez également exécuter des requêtes dans Athena depuis la console Amazon S3.

Utilisation de la console S3 et d'Amazon Athena

La procédure suivante utilise la console Amazon S3 pour accéder à l'éditeur de requêtes Athena afin que vous puissiez interroger une table avec Amazon Athena.

> **Note**
>
> Avant d'effectuer les étapes suivantes, assurez-vous d'avoir intégré vos compartiments de tables aux services AWS d'analyse de cette région. Pour de plus amples informations, veuillez consulter the section called "Utilisation de tables S3 avec des services AWS d'analyse".

Pour interroger une table

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments de tables.
3. Sur la page Compartiments de table, choisissez le compartiment contenant la table que vous souhaitez interroger.
4. Sur la page des détails du bucket, cliquez sur le bouton d'option situé à côté du nom de la table que vous souhaitez interroger.
5. Choisissez Query table with Athena.
6. La console Amazon Athena s'ouvre et l'éditeur de requêtes Athena apparaît avec un exemple `SELECT` de requête chargé pour vous. Modifiez cette requête en fonction de votre cas d'utilisation.

   Dans l'éditeur de requêtes, le champ Catalogue doit être renseigné avec s3tablescatalog/suivi du nom de votre bucket de table, par exemple, s3tablescatalog/***amzn-s3-demo-bucket***. Le champ Base de données doit être renseigné avec l'espace de noms dans lequel votre table est stockée.

   > **Note**
   >
   > Si vous ne voyez pas ces valeurs dans les champs Catalogue et Base de données, assurez-vous d'avoir intégré vos compartiments de tables aux services AWS d'analyse

de cette région. Pour de plus amples informations, veuillez consulter the section called "Utilisation de tables S3 avec des services AWS d'analyse".

7. Pour exécuter la requête, choisissez ensuite Run (Exécuter).

> **Note**
>
> - Si vous recevez le message d'erreur « Autorisations insuffisantes pour exécuter la requête. Le principal n'a aucun privilège sur la ressource spécifiée. » Lorsque vous essayez d'exécuter une requête dans Athena, vous devez obtenir les autorisations Lake Formation nécessaires sur la table. Pour de plus amples informations, veuillez consulter the section called "Octroi d'une autorisation sur une table ou une base de données".
> - Si le message d'erreur « Iceberg ne peut pas accéder à la ressource demandée » s'affiche lorsque vous essayez d'exécuter la requête, accédez à la AWS Lake Formation console et assurez-vous que vous vous êtes accordé des autorisations sur le catalogue de compartiments de tables et la base de données (espace de noms) que vous avez créés. Ne spécifiez pas de table lorsque vous accordez ces autorisations. Pour de plus amples informations, veuillez consulter the section called "Octroi d'une autorisation sur une table ou une base de données".
> - Si vous recevez le message d'erreur suivant lorsque vous exécutez une `SELECT` requête dans Athena, cela est dû à la présence de lettres majuscules dans le nom de votre table ou dans le nom de vos colonnes dans la définition de votre table : « GENERIC_INTERNAL_ERROR : Get table request failed : com.amazonaws.services.glue.model. ValidationException: ressource de fédération non prise en charge - Noms de table ou de colonne non valides. » Assurez-vous que les noms des tables et des colonnes sont tous en minuscules.

Accès aux tables Amazon S3 avec Amazon Redshift

Amazon Redshift est un service d'entrepôt de données rapide, entièrement géré et doté d'une capacité de plusieurs pétaoctets. Il permet d'analyser de manière efficace, simple et économique toutes vos données grâce à vos outils d'informatique décisionnelle existants. Redshift sans serveur vous permet d'accéder aux données et de les analyser sans toutes les configurations d'un entrepôt

de données mis en service. Pour plus d'informations, consultez Commencer avec les entrepôts de données sans serveur dans le Guide de démarrage d'Amazon Redshift.

Interrogez les tables Amazon S3 avec Amazon Redshift

Prérequis

- Intégrez vos compartiments de tables avec les services d'analytique AWS.
  - Création d'un espace de noms.
  - Créer une table .
- Accorder des autorisations à Lake Formation sur les ressources de votre table.

Une fois les prérequis satisfaits, vous pouvez commencer à utiliser Amazon Redshift pour interroger les tables de l'une des manières suivantes :

- En utilisant Amazon Redshift Query Editor v2
- En vous connectant à un entrepôt de données Amazon Redshift à l'aide des outils client SQL
- En utilisant l'API de données Amazon Redshift

Accès aux tables Amazon S3 avec Amazon EMR

Amazon EMR (anciennement Amazon Elastic MapReduce) est une plateforme de clusters gérés qui simplifie l'exécution de frameworks de mégadonnées, tels que le AWS traitement Apache Hadoop et Apache Spark l'analyse de grandes quantités de données. Grâce à ces infrastructures et des projets open source connexes, vous pouvez traiter des données à des fins d'analyse et pour des charges de travail business intelligence. Amazon EMR vous permet également de transformer et de transférer de grandes quantités de données vers et depuis d'autres banques de données et bases de AWS données.

Vous pouvez utiliser des clusters Apache Iceberg dans Amazon EMR pour travailler avec les tables S3 en vous connectant à des compartiments de tables au cours d'une session Spark. Pour vous connecter aux compartiments de tables dans Amazon EMR, vous pouvez utiliser AWS l'intégration des services d'analyse AWS Glue Data Catalog via ou utiliser le catalogue de tables Amazon S3 open source Apache Iceberg pour le catalogue client.

> **Note**
>
> S3 Tables est pris en charge sur Amazon EMR version 7.5 ou supérieure.

Connexion à des compartiments de tables S3 avec Spark sur un cluster Amazon EMR Iceberg

Dans cette procédure, vous configurez un cluster Amazon EMR configuré pour, Apache Iceberg puis vous lancez une Spark session qui se connecte à vos compartiments de table. Vous pouvez le configurer à l'aide de l'intégration des services d' AWS analyse AWS Glue, ou vous pouvez utiliser le catalogue de tables Amazon S3 open source pour Apache Iceberg le catalogue client. Pour obtenir des informations sur le catalogue client, consultez Accès aux tables à l'aide des tables Amazon S3 Iceberg REST point de terminaison.

Choisissez votre méthode d'utilisation des tables avec Amazon EMR parmi les options suivantes.

Amazon S3 Tables Catalog for Apache Iceberg

Les conditions préalables suivantes sont requises pour interroger des tables Spark sur Amazon EMR à l'aide du catalogue de tables Amazon S3 pour. Apache Iceberg

Prérequis

- Attachez la politique `AmazonS3TablesFullAccess` au rôle IAM que vous utilisez pour Amazon EMR.

Pour configurer un cluster Amazon EMR afin d'interroger des tables avec Spark

1. Créez un cluster avec la configuration suivante. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws emr create-cluster --release-label emr-7.5.0 \
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
```

```
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

`configurations.json`:

```
[{
"Classification":"iceberg-defaults",
"Properties":{"iceberg.enabled":"true"}
}]
```

2. Connectez-vous au nœud primaire Spark à l'aide de SSH.
3. Pour initialiser une session Spark pour Iceberg qui se connecte à votre compartiment de tables, entrez la commande suivante. Remplacez le *user input placeholders* par l'ARN de votre bucket de table.

```
spark-shell \
--packages software.amazon.s3tables:s3-tables-catalog-for-iceberg-runtime:0.1.3
 \
--conf spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog \
--conf spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:us-
east-1:111122223333:bucket/amzn-s3-demo-bucket1 \
--conf spark.sql.defaultCatalog=s3tablesbucket \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
```

4. Interrogez vos tables avec Spark SQL. Pour voir des exemples de requêtes, consultez the section called "Interrogation de tables S3 avec Spark SQL".

AWS analytics services integration

Les conditions préalables suivantes sont requises pour interroger des tables Spark sur Amazon EMR à l'aide de AWS l'intégration des services d'analyse.

Prérequis

- Intégrez vos compartiments de table aux services AWS d'analyse.
- Créez le rôle de service par défaut pour Amazon EMR ()`EMR_DefaultRole_V2`. Pour plus de détails, consultez la section Rôle de service pour Amazon EMR (rôle EMR).
- Créez le profil d' EC2 instance Amazon pour Amazon EMR ()`EMR_EC2_DefaultRole`. Pour plus de détails, consultez la section Rôle de service pour les EC2 instances de cluster (profil d'EC2 instance).
  - Joignez la `AmazonS3TablesFullAccess` politique à`EMR_EC2_DefaultRole`.

Pour configurer un cluster Amazon EMR afin d'interroger des tables avec Spark

1. Créez un cluster avec la configuration suivante. Pour utiliser cet exemple, remplacez les *`user input placeholder`* valeurs par vos propres informations.

```
aws emr create-cluster --release-label emr-7.5.0 \
--applications Name=Spark \
--configurations file://configurations.json \
--region us-east-1 \
--name My_Spark_Iceberg_Cluster \
--log-uri s3://amzn-s3-demo-bucket/ \
--instance-type m5.xlarge \
--instance-count 2 \
--service-role EMR_DefaultRole \
--ec2-attributes \

InstanceProfile=EMR_EC2_DefaultRole,SubnetId=subnet-1234567890abcdef0,KeyName=my-key-pair
```

   `configurations.json`:

```
[{
"Classification":"iceberg-defaults",
"Properties":{"iceberg.enabled":"true"}
}]
```

2. Connectez-vous au nœud primaire Spark à l'aide de SSH.
3. Entrez la commande suivante pour initialiser une session Spark pour Iceberg qui se connecte à vos tables. Remplacez *`user input placeholders`* par vos propres informations.

```
spark-shell \
--conf
 spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 \
--conf spark.sql.defaultCatalog=s3tables \
--conf spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog \
--conf spark.sql.catalog.s3tables.catalog-
impl=org.apache.iceberg.aws.glue.GlueCatalog \
--conf spark.sql.catalog.s3tables.client.region=us-east-1 \
--conf spark.sql.catalog.s3tables.glue.id=111122223333
```

4. Interrogez vos tables avec Spark SQL. Pour voir des exemples de requêtes, consultez the section called “Interrogation de tables S3 avec Spark SQL”.

> **Note**
>
> Si vous utilisez la `DROP TABLE PURGE` commande avec Amazon EMR :
>
> - Amazon EMR version 7.5
>
> Définissez la configuration Spark `spark.sql.catalog.`*`your-catalog-name`*`.cache-enabled` sur`false`. Si cette configuration est définie sur `true`, exécutez la commande dans une nouvelle session ou application pour que le cache de table ne soit pas activé.
> - Versions d'Amazon EMR supérieures à 7.5
>
> `DROP TABLE` n'est pas pris en charge. Vous pouvez utiliser l'`DeleteTable`API REST S3 Tables pour supprimer une table.

Visualisation des données d'une table avec QuickSight

QuickSight est un service d'analyse commerciale rapide permettant de créer des visualisations, d'effectuer des analyses ad hoc et d'obtenir rapidement des informations commerciales à partir de vos données. QuickSight découvre facilement AWS les sources de données, permet aux entreprises de s'adapter à des centaines de milliers d'utilisateurs et fournit des performances de requête rapides et réactives grâce au moteur de calcul QuickSight ultrarapide, parallèle, en mémoire (SPICE). Pour plus d'informations, voir Qu'est-ce que c'est QuickSight ? dans le guide de QuickSight l'utilisateur.

Après avoir intégré vos compartiments de tables aux services AWS d'analyse, vous pouvez créer des ensembles de données à partir de vos tables et les QuickSight utiliser à l'aide de SPICE ou de requêtes SQL directes à partir de votre moteur de requêtes. QuickSight prend en charge Athena en tant que source de données pour les tables S3.

Configurer les autorisations QuickSight d'accès aux tables

Avant de travailler avec les données des tables S3, QuickSight vous devez accorder des autorisations au rôle de QuickSight service, à l'utilisateur QuickSight administrateur, et accorder des autorisations Lake Formation sur les tables auxquelles vous souhaitez accéder.

Accorder des autorisations au rôle QuickSight de service

Lorsque vous le configurez QuickSight pour la première fois dans votre compte, il AWS crée un rôle de service qui permet d'accéder QuickSight aux sources de données d'autres AWS services, tels qu'Athena ou Amazon Redshift. Le nom de rôle par défaut est `aws-quicksight-service-role-v0`.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Choisissez Rôles, puis sélectionnez le rôle QuickSight de service. Le nom par défaut est `aws-quicksight-service-role-v0`
3. Choisissez Ajouter des autorisations, puis Créer une politique en ligne.
4. Sélectionnez JSON pour ouvrir l'éditeur de politique JSON, puis ajoutez la politique suivante.

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "glue:GetCatalog",
      "Resource": "*"
    }
  ]
}
```

5. Choisissez Next, entrez un nom de stratégie, puis Create policy.

Pour configurer les autorisations pour l'utilisateur QuickSight administrateur

1. Exécutez la AWS CLI commande suivante pour trouver l'ARN de votre utilisateur QuickSight administrateur.

```
aws quicksight list-users --aws-account-id 111122223333 --namespace default --
region region
```

2. Accordez à Lake Formation des autorisations pour cet ARN. Pour en savoir plus, consultez Accorder des autorisations à Lake Formation sur les ressources de votre table.

Utilisation des données de table dans QuickSight

Vous pouvez vous connecter aux données d'une table en utilisant Athena comme source de données.

Prérequis

- Intégrez vos compartiments de tables avec les services d'analytique AWS.
  - Création d'un espace de noms.
  - Créer une table .
  - Configurer les autorisations QuickSight d'accès aux tables.
- Inscrivez-vous pour QuickSight.

1. Connectez-vous à votre QuickSight compte à l'adresse https://quicksight.aws.amazon.com/
2. Dans le tableau de bord, sélectionnez Nouvelle analyse.
3. Choisissez Nouveau jeu de données.
4. Sélectionnez Athéna.
5. Entrez le nom de la source de données, puis choisissez Créer une source de données.
6. Choisissez Utiliser un SQL personnalisé. Vous ne pourrez pas sélectionner votre table dans le volet Choisissez votre table.
7. Entrez une requête SQL Athena qui capture les colonnes que vous souhaitez visualiser, puis choisissez Confirmer la requête. Par exemple, utilisez la requête suivante pour sélectionner toutes les colonnes :

```
SELECT * FROM "s3tablescatalog/table-bucket-name".namespace.table-name
```

8. Choisissez Visualize pour analyser les données et commencer à créer des tableaux de bord. Pour plus d'informations, voir Visualisation des données dans QuickSight et Exploration de tableaux de bord interactifs dans QuickSight

Diffusion de données vers des tables avec Amazon Data Firehose

Amazon Data Firehose est un service entièrement géré qui fournit des données de streaming en temps réel vers des destinations telles qu'Amazon S3, Amazon Redshift, OpenSearch Amazon Splunk ServiceApache Iceberg, des tables et des points de terminaison HTTP personnalisés ou des points de terminaison HTTP détenus par des fournisseurs de services tiers pris en charge. Avec Amazon Data Firehose, vous n'avez pas besoin d'écrire d'applications ni de gérer de ressources. Vous configurez vos producteurs de données pour envoyer les données à Firehose, qui remet automatiquement les données à la destination que vous avez spécifiée. Vous pouvez également configurer Firehose pour transformer vos données avant de les remettre. Pour en savoir plus sur Amazon Data Firehose, consultez Qu'est-ce qu'Amazon Data Firehose ?

Procédez comme suit pour configurer le streaming Firehose vers des tables situées dans des compartiments de tables S3 :

1. Intégrez vos compartiments de tables avec les services d'analytique AWS.
2. Configurez Firehose pour fournir des données dans vos tables S3. Pour ce faire, vous créez un rôle de service AWS Identity and Access Management (IAM) qui permet à Firehose d'accéder à vos tables.
3. Accordez au rôle de service Firehose des autorisations explicites sur votre table ou son espace de noms. Pour plus d'informations, consultez la section Autorisations de Grant Lake Formation sur les ressources de votre table.
4. Créez un flux Firehose qui achemine les données vers votre table.

Création d'un rôle permettant à Firehose d'utiliser les tables S3 comme destination

Firehose a besoin d'un rôle de service IAM avec des autorisations spécifiques pour accéder aux AWS Glue tables et écrire des données dans les tables S3. Vous devez fournir ce rôle IAM lorsque vous créez un flux Firehose.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, choisissez Politiques.

3. Choisissez Créer une politique, puis JSON dans l'éditeur de politique.
4. Ajoutez la politique en ligne suivante qui accorde des autorisations à toutes les bases de données et tables de votre catalogue de données. Si vous le souhaitez, vous pouvez accorder des autorisations à des tables et à des bases de données spécifiques uniquement. Pour utiliser cette politique, remplacez *user input placeholders* par vos propres informations.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3TableAccessViaGlueFederation",
            "Effect": "Allow",
            "Action": [
                "glue:GetTable",
                "glue:GetDatabase",
                "glue:UpdateTable"
            ],
            "Resource": [
                "arn:aws:glue:us-east-1:account-id:catalog/s3tablescatalog/
*",
                "arn:aws:glue:us-east-1:account-id:catalog/s3tablescatalog",
                "arn:aws:glue:us-east-1:account-id:catalog",
                "arn:aws:glue:us-east-1:account-id:database/*",
                "arn:aws:glue:us-east-1:account-id:table/*/*"
            ]
        },
        {
            "Sid": "S3DeliveryErrorBucketPermission",
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:GetBucketLocation",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject"
            ],
            "Resource": [
                "arn:aws:s3:::error delivery bucket",
                "arn:aws:s3:::error delivery bucket/*"
```

```
            ]
        },
        {
            "Sid": "RequiredWhenUsingKinesisDataStreamsAsSource",
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStream",
                "kinesis:GetShardIterator",
                "kinesis:GetRecords",
                "kinesis:ListShards"
            ],
            "Resource": "arn:aws:kinesis:us-east-1:account-id:stream/stream-
name"
        },
        {
            "Sid":
 "RequiredWhenDoingMetadataReadsANDDataAndMetadataWriteViaLakeformation",
            "Effect": "Allow",
            "Action": [
                "lakeformation:GetDataAccess"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RequiredWhenUsingKMSEncryptionForS3ErrorBucketDelivery",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-1:account-id:key/KMS-key-id"
            ],
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3.us-east-1.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::error
 delivery bucket/prefix*"
                }
            }
        },
        {
```

```
            "Sid": "LoggingInCloudWatch",
            "Effect": "Allow",
            "Action": [
                "logs:PutLogEvents"
            ],
            "Resource": [
                "arn:aws:logs:us-east-1:account-id:log-group:log-group-
name:log-stream:log-stream-name"
            ]
        },
        {
            "Sid": "RequiredWhenAttachingLambdaToFirehose",
            "Effect": "Allow",
            "Action": [
                "lambda:InvokeFunction",
                "lambda:GetFunctionConfiguration"
            ],
            "Resource": [
                "arn:aws:lambda:us-east-1:account-id:function:function-
name:function-version"
            ]
        }
    ]
}
```

Cette politique contient des déclarations qui autorisent l'accès à Kinesis Data Streams, l'invocation des fonctions Lambda et l'accès aux clés. AWS KMS Si vous n'utilisez aucune de ces ressources, vous pouvez supprimer les instructions correspondantes.

Si la journalisation des erreurs est activée, Firehose envoie également des erreurs de livraison de données à votre groupe de CloudWatch journaux et à vos flux. Pour cela, vous devez configurer les noms des flux de journaux et du groupe de journaux. Pour les noms des groupes de journaux et des flux de journaux, consultez Monitor Amazon Data Firehose Using CloudWatch Logs.

5. Une fois que vous avez créé cette politique, créez un rôle IAM avec Service AWS comme Type d'entité approuvée.
6. Pour Service ou cas d'utilisation, choisissez Kinesis. Pour Cas d'utilisation, choisissez Kinesis Firehose.
7. Choisissez Suivant, puis sélectionnez la politique que vous avez créée précédemment.

8. Donnez un nom à votre rôle. Passez en revue les détails de votre rôle, puis choisissez Créer un rôle. Ce rôle sera doté de la politique d'approbation suivante.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
            ],
            "Principal": {
                "Service": [
                    "firehose.amazonaws.com"
                ]
            }
        }
    ]
}
```

Création d'un flux Firehose vers des tables S3

La procédure suivante montre comment créer un flux Firehose pour fournir des données aux tables S3 à l'aide de la console. Les prérequis suivants sont nécessaires pour configurer un flux Firehose vers les tables S3.

Prérequis

- Intégrez vos compartiments de tables avec les services d'analytique AWS.
  - Création d'un espace de noms.
  - Créer une table .
- Créez le rôle permettant à Firehose d'accéder à S3 Tables.
- Accordez à Lake Formation des autorisations sur le rôle de service Firehose que vous avez créé pour accéder aux tables.

Pour fournir des informations de routage à Firehose lorsque vous configurez un flux, vous utilisez votre espace de noms comme nom de base de données et le nom d'une table dans cet espace de noms. Vous pouvez utiliser ces valeurs dans la section Clé unique de la configuration d'un flux Firehose pour router les données vers une table unique. Vous pouvez également utiliser ces valeurs pour router vers une table à l'aide d'expressions de requête JSON. Pour plus d'informations, consultez Routage des enregistrements entrants vers une table Iceberg unique.

Pour configurer un flux Firehose vers les tables S3 (console)

1. Ouvrez la console Firehose à l'adresse. https://console.aws.amazon.com/firehose/
2. Choisissez Créer un flux Firehose.
3. Pour Source, choisissez l'une des sources suivantes :
   - Amazon Kinesis Data Streams
   - Amazon MSK
   - Directement PUT
4. Pour Destination, choisissez Apache IcebergTables.
5. Entrez un nom pour Nom du flux Firehose.
6. Configurez vos Paramètres sources.
7. Pour les paramètres de destination, choisissez Compte courant pour diffuser sur les tables de votre compte ou Compte croisé pour les tables d'un autre compte.
   - Pour les tables du compte courant, sélectionnez votre catalogue de tables S3 dans la liste déroulante Catalogue.
   - Pour les tables d'un compte multicompte, entrez l'ARN du catalogue vers lequel vous souhaitez diffuser des données sur un autre compte.
8. Configurez les noms de base de données et de tables à l'aide d'une configuration de clé unique, d' JSONQuery expressions ou d'une fonction Lambda. Pour plus d'informations, reportez-vous aux sections Router les enregistrements entrants vers une seule table Iceberg et Router les enregistrements entrants vers différentes tables Iceberg du manuel Amazon Data Firehose Developer Guide.
9. Sous Paramètres de sauvegarde, spécifiez un compartiment de sauvegarde S3.
10. Pour Rôles IAM existants, sous Paramètres avancés, sélectionnez le rôle IAM que vous avez créé pour Firehose.
11. Choisissez Créer un flux Firehose.

Pour plus d'informations sur les autres paramètres que vous pouvez configurer pour un flux, consultez Configurer le flux Firehose dans le manuel Amazon Data Firehose Developer Guide.

Exécution de tâches ETL sur des tables Amazon S3 avec AWS Glue

AWS Glue est un service d'intégration de données sans serveur qui permet aux utilisateurs d'outils d'analyse de découvrir, de préparer, de déplacer et d'intégrer facilement des données provenant de sources multiples. Vous pouvez utiliser AWS Glue des tâches pour exécuter des pipelines d'extraction, de transformation et de chargement (ETL) afin de charger des données dans vos lacs de données. Pour plus d'informations AWS Glue, voir Qu'est-ce que c'est AWS Glue ? dans le Guide AWS Glue du développeur.

Une AWS Glue tâche encapsule un script qui se connecte à vos données source, les traite, puis les écrit dans votre cible de données. En général, une tâche exécute les scripts d'extraction, de transformation et de chargement (ETL). Les jobs peuvent exécuter des scripts conçus pour les environnements Apache Spark d'exécution. Vous pouvez surveiller les exécutions de tâche pour comprendre les métriques d'exécution telles que le statut d'achèvement, la durée et l'heure de début.

Vous pouvez utiliser des AWS Glue tâches pour traiter les données de vos tables S3 en vous connectant à vos tables via l'intégration avec les services d' AWS analyse, ou en vous connectant directement à l'aide du point de Iceberg REST terminaison Amazon S3 Tables ou du catalogue de tables Amazon S3 pourApache Iceberg. Ce guide décrit les étapes de base pour commencer à utiliser AWS Glue S3 Tables, notamment :

Rubriques

- Prérequis
- Création d'un script pour se connecter aux compartiments de table
- Création d'une AWS Glue tâche qui interroge des tables

> **Note**
>
> S3 Tables est pris en charge sur AWS Glue la version 5.0 ou supérieure.

Prérequis

Avant de pouvoir interroger des tables à partir AWS Glue d'une tâche, vous devez configurer un rôle IAM qui AWS Glue peut être utilisé pour exécuter la tâche et télécharger le catalogue des tables

Amazon S3 dans un compartiment S3 auquel il AWS Glue peut accéder lors de l'exécution de la tâche. Apache Iceberg JAR

- Intégrez vos compartiments de tables avec les services d'analytique AWS.
- Créez un rôle IAM pour AWS Glue.
  - Associez la politique `AmazonS3TablesFullAccess` gérée au rôle.
  - Associez la politique `AmazonS3FullAccess` gérée au rôle.
- (Facultatif) Si vous utilisez le catalogue des tables Amazon S3, Apache Iceberg vous devez télécharger le catalogue client JAR et le charger dans un compartiment S3.

  Téléchargement du catalogue JAR

  1. Vérifiez la dernière version sur Maven Central. Vous pouvez le télécharger JAR depuis Maven Central à l'aide de votre navigateur ou à l'aide de la commande suivante. Assurez-vous de remplacer le *`version number`* par la dernière version.

     ```
     wget https://repo1.maven.org/maven2/software/amazon/s3tables/s3-tables-catalog-for-iceberg-runtime/0.1.5/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar
     ```

  2. Téléchargez le fichier téléchargé JAR dans un compartiment S3 auquel votre rôle AWS Glue IAM peut accéder. Vous pouvez utiliser la AWS CLI commande suivante pour télécharger leJAR. Assurez-vous de remplacer le *`version number`* par la dernière version et le *`bucket name`* et *`path`* par la vôtre.

     ```
     aws s3 cp s3-tables-catalog-for-iceberg-runtime-0.1.5.jar s3://amzn-s3-demo-bucket/jars/
     ```

Création d'un script pour se connecter aux compartiments de table

Pour accéder aux données de votre table lorsque vous exécutez une tâche AWS Glue ETL, vous configurez une Spark session Apache Iceberg qui se connecte à votre compartiment de table S3. Vous pouvez modifier un script existant pour vous connecter à votre compartiment de table ou créer un nouveau script. Pour plus d'informations sur la création de AWS Glue scripts, consultez Tutoriel : rédaction d'un script AWS Glue pour Spark dans le guide du AWS Glue développeur.

Vous pouvez configurer la session pour vous connecter à vos compartiments de table via l'une des méthodes d'accès aux tables S3 suivantes :

- Intégration de S3 Tables aux services AWS d'analyse
- Point de Iceberg REST terminaison Amazon S3 Tables
- Catalogue de tables Amazon S3 pour Apache Iceberg

Choisissez l'une des méthodes d'accès suivantes pour consulter les instructions de configuration et les exemples de configuration.

AWS analytics services integration

Pour interroger des tables en AWS Glue utilisant l'intégration Spark des services AWS d'analyse, vous devez intégrer vos compartiments de tables aux AWS services d'analyse

Vous pouvez configurer la connexion à votre compartiment de table par le biais d'une Spark session dans le cadre d'une tâche ou par AWS Glue Studio magie dans le cadre d'une session interactive. Pour utiliser les exemples suivants, remplacez les par *`placeholder values`* les informations relatives à votre propre compartiment de table.

Utiliser un PySpark script

Utilisez l'extrait de code suivant dans un PySpark script pour configurer une AWS Glue tâche afin de se connecter à votre compartiment de table à l'aide de l'intégration.

```
spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables") \
    .config("spark.sql.catalog.s3tables",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-
bucket/warehouse/") \
    .getOrCreate()
```

Utilisation d'une AWS Glue session interactive

Si vous utilisez une session de bloc-notes interactive avec la AWS Glue version 5.0, spécifiez les mêmes configurations en utilisant la `%%configure` magie d'une cellule avant l'exécution du code.

```
%%configure
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3tables --conf
 spark.sql.catalog.s3tables=org.apache.iceberg.spark.SparkCatalog --conf
 spark.sql.catalog.s3tables.catalog-impl=org.apache.iceberg.aws.glue.GlueCatalog
 --conf spark.sql.catalog.s3tables.glue.id=111122223333:s3tablescatalog/amzn-s3-
demo-table-bucket --conf spark.sql.catalog.s3tables.warehouse=s3://amzn-s3-demo-
table-bucket/warehouse/"}
```

Amazon S3 Tables Iceberg REST endpoint

Vous pouvez configurer la connexion à votre compartiment de table par le biais d'une Spark session dans le cadre d'une tâche ou par AWS Glue Studio magie dans le cadre d'une session interactive. Pour utiliser les exemples suivants, remplacez les par *`placeholder values`* les informations relatives à votre propre compartiment de table.

Utiliser un PySpark script

Utilisez l'extrait de code suivant dans un PySpark script pour configurer une AWS Glue tâche afin de se connecter à votre compartiment de table à l'aide du point de terminaison.

```
spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:s3tablescatalog/amzn-s3-demo-table-
bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
```

```
    .getOrCreate()
```

Utilisation d'une AWS Glue session interactive

Si vous utilisez une session de bloc-notes interactive avec la AWS Glue version 5.0, spécifiez les mêmes configurations en utilisant la `%%configure` magie d'une cellule avant l'exécution du code. Remplacez les valeurs de l'espace réservé par les informations relatives à votre propre compartiment de table.

```
%%configure
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3_rest_catalog --conf
 spark.sql.catalog.s3_rest_catalog=org.apache.iceberg.spark.SparkCatalog
 --conf spark.sql.catalog.s3_rest_catalog.type=rest --conf
 spark.sql.catalog.s3_rest_catalog.uri=https://s3tables.Region.amazonaws.com/
iceberg --conf
 spark.sql.catalog.s3_rest_catalog.warehouse=arn:aws:s3tables:Region:111122223333:s3table
amzn-s3-demo-table-bucket --conf spark.sql.catalog.s3_rest_catalog.rest.sigv4-
enabled=true --conf spark.sql.catalog.s3_rest_catalog.rest.signing-name=s3tables
 --conf spark.sql.catalog.s3_rest_catalog.rest.signing-region=Region --conf
 spark.sql.catalog.s3_rest_catalog.io-impl=org.apache.iceberg.aws.s3.S3FileIO --
conf spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-enabled=false"}
```

Amazon S3 Tables Catalog for Apache Iceberg

Pour vous connecter à des tables à l'aide du catalogue de tables Amazon S3, Apache Iceberg vous devez d'abord télécharger le dernier fichier jar du catalogue et le charger dans un compartiment S3. Ensuite, lorsque vous créez votre tâche, vous ajoutez le chemin d'accès au catalogue client JAR en tant que paramètre spécial. Pour plus d'informations sur les paramètres des tâches dans AWS Glue, consultez la section Paramètres spéciaux utilisés dans les AWS Glue tâches du Guide du AWS Glue développeur.

Vous pouvez configurer la connexion à votre compartiment de table par le biais d'une Spark session dans le cadre d'une tâche ou par AWS Glue Studio magie dans le cadre d'une session interactive. Pour utiliser les exemples suivants, remplacez les par *`placeholder values`* les informations relatives à votre propre compartiment de table.

Utiliser un PySpark script

Utilisez l'extrait de code suivant dans un PySpark script pour configurer une AWS Glue tâche afin de se connecter à votre compartiment de table à l'aide du. JAR Remplacez les valeurs de l'espace réservé par les informations relatives à votre propre compartiment de table.

```
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()
```

Utilisation d'une AWS Glue session interactive

Si vous utilisez une session de bloc-notes interactive avec la AWS Glue version 5.0, spécifiez les mêmes configurations en utilisant la `%%configure` magie d'une cellule avant l'exécution du code. Remplacez les valeurs de l'espace réservé par les informations relatives à votre propre compartiment de table.

```
%%configure
{"conf":
 "spark.sql.extensions=org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions
 --conf spark.sql.defaultCatalog=s3tablesbucket --conf
 spark.sql.catalog.s3tablesbucket=org.apache.iceberg.spark.SparkCatalog
 --conf spark.sql.catalog.s3tablesbucket.catalog-
impl=software.amazon.s3tables.iceberg.S3TablesCatalog --conf
 spark.sql.catalog.s3tablesbucket.warehouse=arn:aws:s3tables:Region:111122223333:bucket/
amzn-s3-demo-table-bucket", "extra-jars": "s3://amzn-s3-demo-bucket/jars/s3-
tables-catalog-for-iceberg-runtime-0.1.5.jar"}
```

Exemples de scripts

Les exemples de PySpark scripts suivants peuvent être utilisés pour tester l'interrogation des tables S3 avec une AWS Glue tâche. Ces scripts se connectent à votre compartiment de table et exécutent des requêtes pour : créer un nouvel espace de noms, créer un exemple de table, insérer

des données dans la table et renvoyer les données de la table. Pour utiliser les scripts, remplacez-les par *placeholder values* les informations relatives à votre propre compartiment de table.

Choisissez parmi les scripts suivants en fonction de votre méthode d'accès aux tables S3.

S3 Tables integration with AWS analytics services

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("SparkIcebergSQL") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog","s3tables")
    .config("spark.sql.catalog.s3tables", "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tables.catalog-impl",
 "org.apache.iceberg.aws.glue.GlueCatalog") \
    .config("spark.sql.catalog.s3tables.glue.id",
 "111122223333:s3tablescatalog/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3tables.warehouse", "s3://amzn-s3-demo-table-bucket/
bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

namespace = "new_namespace"
table = "new_table"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")
```

```
spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Amazon S3 Tables Iceberg REST endpoint

```
from pyspark.sql import SparkSession

spark = SparkSession.builder.appName("glue-s3-tables-rest") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3_rest_catalog") \
    .config("spark.sql.catalog.s3_rest_catalog",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3_rest_catalog.type", "rest") \
    .config("spark.sql.catalog.s3_rest_catalog.uri", "https://
s3tables.Region.amazonaws.com/iceberg") \
    .config("spark.sql.catalog.s3_rest_catalog.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.sigv4-enabled", "true") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-name", "s3tables") \
    .config("spark.sql.catalog.s3_rest_catalog.rest.signing-region", "Region") \
    .config('spark.sql.catalog.s3_rest_catalog.io-
impl','org.apache.iceberg.aws.s3.S3FileIO') \
    .config('spark.sql.catalog.s3_rest_catalog.rest-metrics-reporting-
enabled','false') \
    .getOrCreate()

namespace = "s3_tables_rest_namespace"
table = "new_table_s3_rest"

spark.sql("SHOW DATABASES").show()

spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
```

```
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Amazon S3 Tables Catalog for Apache Iceberg

```
from pyspark.sql import SparkSession

#Spark session configurations
spark = SparkSession.builder.appName("glue-s3-tables") \
    .config("spark.sql.extensions",
 "org.apache.iceberg.spark.extensions.IcebergSparkSessionExtensions") \
    .config("spark.sql.defaultCatalog", "s3tablesbucket") \
    .config("spark.sql.catalog.s3tablesbucket",
 "org.apache.iceberg.spark.SparkCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.catalog-impl",
 "software.amazon.s3tables.iceberg.S3TablesCatalog") \
    .config("spark.sql.catalog.s3tablesbucket.warehouse",
 "arn:aws:s3tables:Region:111122223333:bucket/amzn-s3-demo-table-bucket") \
    .getOrCreate()

#Script
namespace = "new_namespace"
table = "new_table"

spark.sql(f"CREATE NAMESPACE IF NOT EXISTS s3tablesbucket.{namespace}")
spark.sql(f"DESCRIBE NAMESPACE {namespace}").show()

spark.sql(f"""
    CREATE TABLE IF NOT EXISTS {namespace}.{table} (
       id INT,
       name STRING,
       value INT
    )
""")

spark.sql(f"""
    INSERT INTO {namespace}.{table}
```

```
    VALUES
       (1, 'ABC', 100),
       (2, 'XYZ', 200)
""")

spark.sql(f"SELECT * FROM {namespace}.{table} LIMIT 10").show()
```

Création d'une AWS Glue tâche qui interroge des tables

Les procédures suivantes indiquent comment configurer des AWS Glue tâches qui se connectent à vos compartiments de table S3. Vous pouvez le faire en utilisant AWS CLI ou en utilisant la console avec l'éditeur de AWS Glue Studio script. Pour plus d'informations, consultez la section Création de tâches AWS Glue dans le Guide de l'AWS Glue utilisateur.

Utilisation de l'éditeur de AWS Glue Studio script

La procédure suivante montre comment utiliser l'éditeur de AWS Glue Studio script pour créer une tâche ETL qui interroge vos tables S3.

Prérequis

- Prérequis
- Création d'un script pour se connecter aux compartiments de table

1. Ouvrez la AWS Glue console à l'adresse https://console.aws.amazon.com/glue/.
2. Dans le volet de navigation, sélectionnez ETL jobs.
3. Choisissez l'éditeur de script, puis choisissez Upload script et téléchargez le PySpark script que vous avez créé pour interroger les tables S3.
4. Sélectionnez l'onglet Détails du Job et entrez les informations suivantes pour les propriétés de base.
   - Dans Nom, entrez le nom de la tâche.
   - Pour le rôle IAM, sélectionnez le rôle pour AWS Glue lequel vous avez créé.
5. (Facultatif) Si vous utilisez le catalogue de tables Amazon S3 pour la méthode Apache Iceberg d'accès, pour étendre les propriétés avancées et pour le JARs chemin dépendant, entrez l'URI S3 du fichier jar du catalogue client que vous avez chargé dans un compartiment S3 comme

condition préalable. Par exemple, s3 ://*amzn-s3-demo-bucket1*/*jars*/s3- tables-catalog-for-iceberg -runtime- .jar *0.1.5*

6. Choisissez Enregistrer pour créer la tâche.
7. Choisissez Exécuter, lancez la tâche et vérifiez l'état de la tâche sous l'onglet Exécutions.

En utilisant le AWS CLI

La procédure suivante montre comment utiliser le AWS CLI pour créer une tâche ETL qui interroge vos tables S3. Pour utiliser les commandes, remplacez-les *placeholder values* par les vôtres.

Prérequis

- Prérequis
- Création d'un script pour se connecter aux compartiments de tableet chargez-le dans un compartiment S3.

1. Créez un AWS Glue emploi.

```
aws glue create-job \
--name etl-tables-job \
--role arn:aws:iam::111122223333:role/AWSGlueServiceRole \
--command '{
    "Name": "glueetl",
    "ScriptLocation": "s3://amzn-s3-demo-bucket1/scripts/glue-etl-query.py",
    "PythonVersion": "3"
}' \
--default-arguments '{
    "--job-language": "python",
    "--class": "GlueApp"
}' \
--glue-version "5.0"
```

> **Note**
>
> (Facultatif) Si vous utilisez le catalogue des tables Amazon S3 Apache Iceberg comme méthode d'accès, ajoutez le catalogue client JAR au `--extra-jars` paramètre `--default-arguments` using the. Remplacez le *input placeholders* par le vôtre lorsque vous ajoutez le paramètre.

```
                        "--extra-jars": "s3://amzn-s3-demo-bucket/jar-
path/s3-tables-catalog-for-iceberg-runtime-0.1.5.jar"
```

2. Commencez votre travail.

```
aws glue start-job-run \
--job-name etl-tables-job
```

3. Pour vérifier l'état de votre tâche, copiez l'ID d'exécution de la commande précédente et saisissez-le dans la commande suivante.

```
aws glue get-job-run --job-name etl-tables-job \
--run-id jr_ec9a8a302e71f8483060f87b6c309601ea9ee9c1ffc2db56706dfcceb3d0e1ad
```

Tables S3 Régions AWS, points de terminaison et quotas de service

Les sections suivantes présentent les quotas de service Régions AWS et les quotas de service pris en charge pour les tables S3.

Rubriques

- Tables Régions AWS et points de terminaison S3
- Quotas des tables S3

Tables Régions AWS et points de terminaison S3

Pour une liste des régions dans lesquelles S3 Tables est actuellement disponible, consultez Amazon S3 endpoints. Pour vous connecter par programmation à un AWS service, vous utilisez un point de terminaison. Pour plus d'informations, consultez Points de terminaison du service AWS. Pour plus d'informations sur les points de terminaison Amazon S3, consultez Points de terminaison Amazon S3.

Nom de la région	Région	Point de terminaison	Protocole	Prise en charge de(s) version(s) de signature
Afrique (Le Cap)	af-south-1	`s3tables.af-south-1.amazonaws.com`	HTTPS	4
Asie-Pacifique (Hong Kong)	ap-east-1	`s3tables.ap-east-1.amazonaws.com`	HTTPS	4
Asie-Pacifique (Tokyo)	ap-northeast-1	`s3tables.ap-northeast-1.amazonaws.com`	HTTPS	4
Asia Pacific (Seoul)	ap-northeast-2	`s3tables.ap-northeast-2.amazonaws.com`	HTTPS	4
Asie-Pacifique (Osaka)	ap-northeast-3	`s3tables.ap-northeast-3.amazonaws.com`	HTTPS	4
Asia Pacific (Mumbai)	ap-south-1	`s3tables.ap-south-1.amazonaws.com`	HTTPS	4
Asie-Pacifique (Hyderabad)	ap-south-2	`s3tables.ap-south-`	HTTPS	4

Nom de la région	Région	Point de terminaison	Protocole	Prise en charge de(s) version(s) de signature
		2.amazonaws.com		
Asie-Pacifique (Singapour)	ap-southeast-1	s3tables.ap-southeast-1.amazonaws.com	HTTPS	4
Asie-Pacifique (Sydney)	ap-southeast-2	s3tables.ap-southeast-2.amazonaws.com	HTTPS	4
Asie-Pacifique (Jakarta)	ap-southeast-3	s3tables.ap-southeast-3.amazonaws.com	HTTPS	4
Asie-Pacifique (Melbourne)	ap-southeast-4	s3tables.ap-southeast-4.amazonaws.com	HTTPS	4
Asie-Pacifique (Malaisie)	ap-southeast-5	s3tables.ap-southeast-5.amazonaws.com	HTTPS	4
Asie-Pacifique (Thaïlande)	ap-sud-est 7	s3tables.ap-southeast-7.amazonaws.com	HTTPS	4

Nom de la région	Région	Point de terminaison	Protocole	Prise en charge de(s) version(s) de signature
Canada (Centre)	ca-central-1	`s3tables.ca-central-1.amazonaws.com`	HTTPS	4
Canada Ouest (Calgary)	ca-west-1	`s3tables.ca-west-1.amazonaws.com`	HTTPS	4
Europe (Francfort)	eu-central-1	`s3tables.eu-central-1.amazonaws.com`	HTTPS	4
Europe (Zurich)	eu-central-2	`s3tables.eu-central-2.amazonaws.com`	HTTPS	4
Europe (Stockholm)	eu-north-1	`s3tables.eu-north-1.amazonaws.com`	HTTPS	4
Europe (Milan)	eu-south-1	`s3tables.eu-south-1.amazonaws.com`	HTTPS	4
Europe (Espagne)	eu-south-2	`s3tables.eu-south-2.amazonaws.com`	HTTPS	4

Nom de la région	Région	Point de terminaison	Protocole	Prise en charge de(s) version(s) de signature
Europe (Irlande)	eu-west-1	`s3tables.eu-west-1.amazonaws.com`	HTTPS	4
Europe (Londres)	eu-west-2	`s3tables.eu-west-2.amazonaws.com`	HTTPS	4
Europe (Paris)	eu-west-3	`s3tables.eu-west-3.amazonaws.com`	HTTPS	4
Israël (Tel Aviv)	il-central-1	`s3tables.il-central-1.amazonaws.com`	HTTPS	4
Moyen-Orient (EAU)	me-central-1	`s3tables.me-central-1.amazonaws.com`	HTTPS	4
Moyen-Orient (Bahreïn)	me-south-1	`s3tables.me-south-1.amazonaws.com`	HTTPS	4
Mexique (centre)	mx-central-1	`s3tables.mx-central-1.amazonaws.com`	HTTPS	4

Nom de la région	Région	Point de terminaison	Protocole	Prise en charge de(s) version(s) de signature
Amérique du Sud (Sao Paulo)	sa-east-1	`s3tables.sa-east-1.amazonaws.com`	HTTPS	4
US East (N. Virginia)	us-east-1	`s3tables.us-east-1.amazonaws.com`	HTTPS	4
USA Est (Ohio)	us-east-2	`s3tables.us-east-2.amazonaws.com`	HTTPS	4
USA Ouest (Californie du Nord)	us-west-1	`s3tables.us-west-1.amazonaws.com`	HTTPS	4
USA Ouest (Oregon)	us-west-2	`s3tables.us-west-2.amazonaws.com`	HTTPS	4

Quotas des tables S3

Les quotas, également appelés limites, sont le nombre maximum de ressources de service ou d'opérations pour vous Compte AWS. Les quotas pour les ressources des tables S3 sont les suivants. Pour plus d'informations sur les quotas Amazon S3, consultez la section Quotas Amazon S3.

Nom	Par défaut	Ajustable	Description
Compartiments de tables	10	Pour demander une augmentation de quota, contactez Support.	Le nombre de compartiments de table Amazon S3 que vous pouvez créer par Région AWS compte.
Espaces de noms	10 000	Pour demander une augmentation de quota, contactez Support.	Nombre de compartiments de tables Amazon S3 que vous pouvez créer par compartiment de tables.
Tables	10 000	Pour demander une augmentation de quota, contactez Support.	Nombre de tables Amazon S3 que vous pouvez créer par compartiment de tables.

Sécurité pour S3 Tables

Amazon S3 fournit plusieurs fonctionnalités et outils de sécurité. Vous trouverez ci-dessous une liste des fonctionnalités et outils pris en charge par S3 Tables. Une utilisation correcte de ces outils peut contribuer à garantir que vos ressources sont protégées et accessibles uniquement aux utilisateurs prévus.

Politiques basées sur l'identité

Les politiques basées sur une identité sont attachées à un utilisateur, un groupe ou un rôle IAM. Vous pouvez utiliser des politiques basées sur l'identité pour accorder à une identité IAM l'accès à vos tables et compartiments de tables. Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ni modifier les tables et les compartiments de tables. Ils ne peuvent pas non plus effectuer de tâches à l'aide de la console S3 ou d'Amazon S3 REST APIs. AWS CLI Vous pouvez créer des utilisateurs, des groupes et des rôles IAM dans votre compte et leur attacher des stratégies d'accès. Vous pouvez alors accorder l'accès à vos ressources. Pour créer des compartiments de tables et

des tables et y accéder, un administrateur IAM doit accorder les autorisations nécessaires au rôle AWS Identity and Access Management (IAM) ou aux utilisateurs. Pour plus d'informations, consultez Gestion des accès pour S3 Tables.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont attachées à une ressource. Vous pouvez créer des politiques basées sur les ressources pour les tables et les compartiments de tables. Vous pouvez utiliser une politique de compartiment de tables pour contrôler les autorisations d'accès de l'API au niveau du compartiment de tables et de l'espace de noms. Vous pouvez également utiliser une politique de compartiment de tables pour contrôler les autorisations de l'API au niveau de la table sur plusieurs tables d'un compartiment. Selon la définition de la politique, les autorisations attachées au compartiment peuvent s'appliquer à toutes les tables du compartiment ou à des tables spécifiques du compartiment. Vous pouvez également utiliser une politique de tables pour accorder des autorisations d'accès de l'API au niveau de la table à des tables individuelles du compartiment.

Lorsque le service S3 Tables reçoit une demande pour effectuer une opération de compartiment de tables ou une opération de table, il commence par vérifier que le demandeur possède les autorisations nécessaires. Il évalue toutes les stratégies d'accès pertinentes, les politiques utilisateur et les politiques basées sur les ressources pour décider d'autoriser ou non la demande (politique utilisateur IAM, politique de rôle IAM, politique de compartiment de tables et politique de tables). Avec les politiques de compartiments de tables et les politiques de tables, vous pouvez personnaliser l'accès à vos ressources pour vous assurer que seules les identités que vous avez approuvées peuvent accéder à vos ressources et réaliser des actions sur ces dernières. Pour plus d'informations, consultez Gestion des accès pour S3 Tables.

AWS Organizations politiques de contrôle des services (SCPs) pour les tables S3.

Vous pouvez utiliser les tables Amazon S3 dans les politiques de contrôle des services (SCPs) pour gérer les autorisations accordées aux utilisateurs de votre organisation. À l'instar des politiques IAM et des ressources, toutes les actions au niveau des tables et des compartiments sont référencées dans le cadre de l'espace de `s3tables` noms des politiques. Pour plus d'informations, voir Politiques de contrôle des services (SCPs) dans le guide de AWS Organizations l'utilisateur.

Rubriques

- Protection des données des tables S3 grâce au chiffrement
- Gestion des accès pour S3 Tables
- Connectivité VPC pour les tables S3

- Considérations et restrictions de sécurité pour S3 Tables

Protection des données des tables S3 grâce au chiffrement

Utilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de tables

Rubriques

- Comment fonctionne SSE-KMS pour les tables et les seaux de table
- Application et définition de l'utilisation du SSE-KMS pour les tables et les compartiments de tables
- Surveillance et audit du chiffrement SSE-KMS pour les tables et les compartiments de tables
- Exigences d'autorisation pour le chiffrement SSE-KMS des tables S3
- Spécification du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS) dans des compartiments de table

Les compartiments de tables ont une configuration de chiffrement par défaut qui chiffre automatiquement les tables en utilisant le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Ce chiffrement s'applique à toutes les tables de vos compartiments de tables S3 et est gratuit pour vous.

Si vous avez besoin d'un contrôle accru sur vos clés de chiffrement, par exemple pour gérer la rotation des clés et l'attribution des politiques d'accès, vous pouvez configurer vos compartiments de table pour utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Les contrôles de sécurité intégrés AWS KMS peuvent vous aider à respecter les exigences de conformité liées au chiffrement. Pour en savoir plus sur SSE-KMS, consultez Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

Comment fonctionne SSE-KMS pour les tables et les seaux de table

Le SSE-KMS avec compartiments de table se distingue du SSE-KMS en ce qui concerne les compartiments à usage général des manières suivantes :

- Vous pouvez définir les paramètres de chiffrement pour les compartiments de tables et les tables individuelles.
- Vous ne pouvez utiliser des clés gérées par le client qu'avec SSE-KMS. AWS les clés gérées ne sont pas prises en charge.

- Vous devez accorder des autorisations à certains rôles et à certains responsables AWS de service pour accéder à votre AWS KMS clé. Pour de plus amples informations, veuillez consulter Exigences d'autorisation pour le chiffrement SSE-KMS des tables S3. Cela inclut l'octroi de l'accès à :
  - Le principe de maintenance S3 : pour effectuer la maintenance des tables sur des tables chiffrées
  - Votre rôle d'intégration des tables S3 : pour travailler avec des tables chiffrées dans les services AWS d'analyse
  - Votre rôle d'accès client : pour un accès direct aux tables chiffrées des Apache Iceberg clients
  - Le principe des métadonnées S3 : pour mettre à jour les tables de métadonnées S3 cryptées
- Les tables chiffrées utilisent des clés au niveau des tables qui minimisent le nombre de demandes afin de AWS KMS rendre l'utilisation des tables chiffrées SSE-KMS plus rentable.

Chiffrement SSE-KMS pour les compartiments de tables

Lorsque vous créez un bucket de table, vous pouvez choisir SSE-KMS comme type de chiffrement par défaut et sélectionner une clé KMS spécifique qui sera utilisée pour le chiffrement. Toutes les tables créées dans ce compartiment hériteront automatiquement de ces paramètres de chiffrement de leur compartiment de table. Vous pouvez utiliser l' AWS CLI API S3 ou modifier ou AWS SDKs supprimer les paramètres de chiffrement par défaut d'un bucket de table à tout moment. Lorsque vous modifiez les paramètres de chiffrement d'un compartiment de tables, ces paramètres s'appliquent uniquement aux nouvelles tables créées dans ce compartiment. Les paramètres de chiffrement des tables préexistantes ne sont pas modifiés. Pour de plus amples informations, veuillez consulter Spécification du chiffrement pour les compartiments de tables.

Chiffrement SSE-KMS pour les tables

Vous avez également la possibilité de chiffrer une table individuelle avec une clé KMS différente, quelle que soit la configuration de chiffrement par défaut du compartiment. Pour définir le chiffrement d'une table individuelle, vous devez spécifier la clé de chiffrement souhaitée au moment de la création de la table. Si vous souhaitez modifier le chiffrement d'une table existante, vous devez créer une table avec la clé souhaitée et copier les données de l'ancienne table vers la nouvelle. Pour de plus amples informations, veuillez consulter Spécification du chiffrement pour les tables.

Lorsque AWS KMS le chiffrement est utilisé, S3 Tables crée automatiquement des clés de données uniques au niveau des tables qui chiffrent les nouveaux objets associés à chaque table. Ces clés

sont utilisées pendant une période limitée, ce qui permet de minimiser le besoin de AWS KMS demandes supplémentaires lors des opérations de chiffrement et de réduire le coût du chiffrement. Ceci est similaire àClés de compartiment S3 pour SSE-KMS.

Application et définition de l'utilisation du SSE-KMS pour les tables et les compartiments de tables

Vous pouvez utiliser les politiques basées sur les ressources de S3 Tables, les politiques clés KMS, les politiques basées sur l'identité IAM, ou toute combinaison de celles-ci, pour imposer l'utilisation de SSE-KMS pour les tables S3 et les compartiments de tables. Pour plus d'informations sur les politiques d'identité et de ressources pour les tables, consultezGestion des accès pour S3 Tables. Pour plus d'informations sur la rédaction de politiques clés, consultez la section Politiques clés du Guide du AWS Key Management Service développeur. Les exemples suivants montrent comment vous pouvez utiliser des politiques pour appliquer le SSE-KMS.

Application de l'utilisation de SSE-KMS pour toutes les tables avec une politique de compartiment de tables

Il s'agit d'un exemple de politique de compartiment de tables qui empêche les utilisateurs de créer des tables dans un compartiment de tables spécifique à moins qu'ils ne chiffrent les tables avec une AWS KMS clé spécifique. Pour utiliser cette politique, remplacez-la *user input placeholders* par vos propres informations :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceKMSEncryption",
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3tables:CreateTable"
      ],
      "Resource": [
        "arn:aws:s3tables:us-west-2:111122223333:bucket/example-table-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "s3tables:sseAlgorithm": "aws:kms",
```

```
            "s3tables:kmsKeyArn": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
          }
        }
      }
    ]
}
```

Obliger les utilisateurs à utiliser le chiffrement SSE-KMS avec une politique IAM

Cette politique d'identité IAM oblige les utilisateurs à utiliser une AWS KMS clé spécifique pour le chiffrement lors de la création ou de la configuration des ressources des tables S3. Pour utiliser cette politique, remplacez-la *user input placeholders* par vos propres informations :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "RequireKMSKeyOnTables",
      "Action": [
          "s3tables:CreateTableBucket",
          "s3tables:PutTableBucketEncryption",
          "s3tables:CreateTable"
      ]
      "Effect": "Deny",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
            "s3tables:sseAlgorithm": "aws:kms",
            "s3tables:kmsKeyArn": "<key_arn>"
        }
      }
    }
  ]
}
```

Restreindre l'utilisation d'une clé à un compartiment de table spécifique avec une politique de clé KMS

Cet exemple de politique de clé KMS permet à un utilisateur spécifique d'utiliser la clé uniquement pour les opérations de chiffrement dans un compartiment de table spécifique. Ce type de politique

est utile pour limiter l'accès à une clé dans les scénarios entre comptes. Pour utiliser cette politique, remplacez-la *user input placeholders* par vos propres informations :

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Id",
  "Statement": [
    {
      "Sid": "AllowPermissionsToKMS",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "kms:EncryptionContext:aws:s3:arn": "<table-bucket-arn>/*"
        }
      }
    }
  ]
}
```

Surveillance et audit du chiffrement SSE-KMS pour les tables et les compartiments de tables

Pour vérifier l'utilisation de vos AWS KMS clés pour vos données cryptées SSE-KMS, vous pouvez utiliser AWS CloudTrail des journaux. Vous pouvez obtenir un aperçu de vos opérations cryptographiques, telles que `GenerateDataKey` et`Decrypt`. CloudTrail prend en charge de nombreuses valeurs d'attribut pour filtrer votre recherche, notamment le nom de l'événement, le nom d'utilisateur et la source de l'événement.

Vous pouvez suivre les demandes de configuration de chiffrement pour les tables et les compartiments de tables Amazon S3 à l'aide d' CloudTrail événements. Les noms d'événements d'API suivants sont utilisés dans CloudTrail les journaux :

- `s3tables:PutTableBucketEncryption`
- `s3tables:GetTableBucketEncryption`
- `s3tables:DeleteTableBucketEncryption`
- `s3tables:GetTableEncryption`
- `s3tables:CreateTable`
- `s3tables:CreateTableBucket`

> **Note**
>
> EventBridge n'est pas compatible avec les compartiments de table.

Exigences d'autorisation pour le chiffrement SSE-KMS des tables S3

Lorsque vous utilisez le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) pour les tables des compartiments de tables S3, vous devez accorder des autorisations pour les différentes identités de votre compte. Au minimum, votre identité d'accès et le responsable de maintenance de S3 Tables doivent avoir accès à votre clé, les autres autorisations requises dépendent de votre cas d'utilisation.

Autorisations nécessaires

Pour accéder à une table chiffrée avec une clé KMS, vous devez disposer des autorisations suivantes sur cette clé :

- `kms:GenerateDataKey`
- `kms:Decrypt`

> **Important**
>
> Pour utiliser SSE-KMS sur des tables, le principal du service de maintenance des tables Amazon S3 (`maintenance.s3tables.amazonaws.com`) a besoin `kms:GenerateDataKey` d'`kms:Decrypt`autorisations sur la clé.

Autorisations supplémentaires

Ces autorisations supplémentaires sont requises en fonction de votre cas d'utilisation :

- Autorisations pour l'intégration des services d' AWS analyse : si vous utilisez des tables chiffrées SSE-KMS dans les services AWS d'analyse, votre rôle d'intégration doit être autorisé à utiliser votre clé KMS.
- Autorisations d'accès direct — Si vous travaillez directement avec des tables chiffrées SSE-KMS, par le biais de méthodes telles que le point de Iceberg REST terminaison Amazon S3 Tables ou le catalogue de tables Amazon S3 pourApache Iceberg, vous devez autoriser le rôle IAM utilisé par votre client à accéder à votre clé.
- Autorisations pour les tables de métadonnées S3 — Si vous utilisez le chiffrement SSE-KMS pour les tables de métadonnées S3, vous devez fournir au service de métadonnées S3 l'accès principal (`metadata.s3.amazonaws.com`) à votre clé KMS. Cela permet aux métadonnées S3 de mettre à jour les tables chiffrées afin qu'elles reflètent vos dernières modifications de données.

> **Note**
>
> Pour les clés KMS entre comptes, votre rôle IAM nécessite à la fois une autorisation d'accès par clé et une autorisation explicite dans la politique des clés. Pour plus d'informations sur les autorisations entre comptes pour les clés KMS, voir Autoriser les AWS comptes externes à utiliser une clé KMS dans le Guide du développeur AWS Key Management Service de services.

Rubriques

- Octroi des autorisations principales au service de maintenance S3 Tables sur votre clé KMS
- Octroi aux principaux IAM des autorisations leur permettant de travailler avec des tables chiffrées dans les services d'analyse intégrés AWS
- Octroi aux principaux IAM des autorisations leur permettant de travailler directement avec des tables chiffrées
- Octroi au service de métadonnées S3 des autorisations principales pour utiliser votre clé KMS

Octroi des autorisations principales au service de maintenance S3 Tables sur votre clé KMS

Cette autorisation est requise pour créer des tables chiffrées SSE-KMS et pour permettre la maintenance automatique des tables, comme le compactage, la gestion des instantanés et la suppression de fichiers non référencés sur les tables chiffrées.

> **Note**
>
> Chaque fois que vous demandez la création d'une table cryptée SSE-KMS, S3 Tables vérifie que le `maintenance.s3tables.amazonaws.com` principal a accès à votre clé KMS. Pour effectuer cette vérification, un objet de zéro octet est temporairement créé dans votre compartiment de table. Cet objet sera automatiquement supprimé par les opérations de maintenance de suppression de fichiers non référencés. Si la clé KMS que vous avez spécifiée pour le chiffrement ne dispose pas d'un accès de maintenance, l'opération CreateTable échouera.

Pour accorder un accès de maintenance aux tables chiffrées SSE-KMS, vous pouvez utiliser l'exemple de politique de clé suivant. Dans cette politique, le principal du `maintenance.s3tables.amazonaws.com` service est autorisé à utiliser une clé KMS spécifique pour chiffrer et déchiffrer les tables d'un compartiment de tables spécifique. Pour utiliser cette politique, remplacez-la *`user input placeholders`* par vos propres informations :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": "maintenance.s3tables.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:aws-region:111122223333:key/key-id",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn":"<table-or-table-bucket-
arn>/*"
                }
            }
        }
```

```
    ]
}
```

Octroi aux principaux IAM des autorisations leur permettant de travailler avec des tables chiffrées dans les services d'analyse intégrés AWS

Pour utiliser les tables S3 dans les services AWS d'analyse, vous devez intégrer vos compartiments de tables à Amazon SageMaker Lakehouse. Cette intégration permet aux services AWS d'analyse de découvrir et d'accéder automatiquement aux données des tables. Pour plus d'informations sur l'intégration, consultezUtilisation d'Amazon S3 Tables avec des services AWS d'analyse.

Lorsque vous utilisez des tables chiffrées SSE-KMS dans ces services, le rôle que vous utilisez doit être autorisé à utiliser votre AWS KMS clé pour les opérations de chiffrement. Vous pouvez appliquer ces autorisations au `S3TablesRoleForLakeFormation` rôle créé lors de l'intégration ou à votre propre rôle IAM.

L'exemple de politique IAM intégrée suivant peut être utilisé pour accorder au rôle de `S3TablesRoleForLakeFormation` service l'autorisation d'utiliser une clé KMS spécifique dans votre compte pour les opérations de chiffrement. Pour utiliser cette politique, remplacez-la *`input placeholder values`* par la vôtre.

```
{
  "Sid": "AllowTableRoleAccess",
  "Effect": "Allow",
  "Principal": {
 "AWS": "arn:aws:iam::111122223333:role/service-role/S3TablesRoleForLakeFormation"
  },
  "Action": [
      "kms:GenerateDataKey",
      "kms:Decrypt"
  ],
  "Resource": "<kms-key-arn>"
}
```

Octroi aux principaux IAM des autorisations leur permettant de travailler directement avec des tables chiffrées

Lorsque vous travaillez avec des tables chiffrées à l'aide de méthodes tierces ou d'accès direct, vous devez accorder au rôle que vous utilisez l'accès à votre clé KMS. Les exemples suivants montrent comment accorder l'accès par le biais d'une politique IAM ou d'une politique de clé KMS.

IAM policy

Associez cette politique intégrée à votre rôle IAM pour autoriser l'accès aux clés KMS. Pour utiliser cette politique, *input placeholder values* remplacez-la par votre propre code KMS.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowKMSKeyUsage",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
        }
    ]
}
```

KMS key policy

Associez cette politique intégrée à une clé KMS pour autoriser le AWS KMS rôle spécifié à utiliser la clé. Pour utiliser cette politique, remplacez le *input placeholder values* par votre rôle IAM.

```
{
    "Sid": "Allow use of the key",
    "Effect": "Allow",
    "Principal": {
        "AWS": [
            "arn:aws:iam::<catalog-account-id>:role/<role-name>"
        ]
    },
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey",
    ],
```

```
    "Resource": "*"
}
```

Octroi au service de métadonnées S3 des autorisations principales pour utiliser votre clé KMS

Pour permettre à Amazon S3 de mettre à jour les tables de métadonnées chiffrées SSE-KMS et d'effectuer la maintenance de ces tables de métadonnées, vous pouvez utiliser l'exemple de politique clé suivant. Dans cette politique, vous autorisez les responsables `metadata.s3.amazonaws.com` et les responsables du `maintenance.s3tables.amazonaws.com` service à chiffrer et à déchiffrer les tables d'un compartiment de tables spécifique à l'aide d'une clé spécifique. Pour utiliser cette politique, remplacez-la *`user input placeholders`* par vos propres informations :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EnableKeyUsage",
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "maintenance.s3tables.amazonaws.com",
                    "metadata.s3.amazonaws.com"
                ]
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:us-
west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab",
            "Condition": {
                "StringLike": {
                    "kms:EncryptionContext:aws:s3:arn":"<table-or-table-bucket-
arn>/*"
                }
            }
        }
    ]
```

```
}
```

Spécification du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS) dans des compartiments de table

Le chiffrement est configuré par défaut pour tous les compartiments de table Amazon S3, et toutes les nouvelles tables créées dans un compartiment de table sont automatiquement chiffrées au repos. Le chiffrement côté serveur avec les clés gérées Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment de table. Si vous souhaitez spécifier un autre type de chiffrement, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS).

Vous pouvez spécifier le chiffrement SSE-KMS dans vos `CreateTable` demandes `CreateTableBucket` or, ou vous pouvez définir la configuration de chiffrement par défaut dans le compartiment de table d'une `PutTableBucketEncryption` demande.

> **Important**
>
> Pour autoriser la maintenance automatique des tables et des compartiments de tables chiffrés SSE-KMS, vous devez accorder au principal du service maintenance.s3tables.amazonaws.com l'autorisation d'utiliser votre clé KMS. Pour de plus amples informations, veuillez consulter Exigences d'autorisation pour le chiffrement SSE-KMS des tables S3.

Spécification du chiffrement pour les compartiments de tables

Vous pouvez spécifier SSE-KMS comme type de chiffrement par défaut lorsque vous créez un nouveau bucket de table, voir par exemple. Création d'un compartiment de tables Après avoir créé un bucket de table, vous pouvez spécifier l'utilisation de SSE-KMS comme paramètre de chiffrement par défaut à l'aide des opérations de l'API REST AWS SDKs, et du AWS Command Line Interface ()AWS CLI.

> **Note**
>
> Lorsque vous spécifiez SSE-KMS comme type de chiffrement par défaut, la clé que vous utilisez pour le chiffrement doit autoriser l'accès au principal du service de maintenance des tables S3. Si le principal du service de maintenance n'y a pas accès, vous ne pourrez

pas créer de tables dans ce bucket de tables. Pour de plus amples informations, veuillez consulter Octroi des autorisations principales au service de maintenance S3 Tables sur votre clé KMS .

En utilisant le AWS CLI

Pour utiliser l'exemple de AWS CLI commande suivant, remplacez le *user input placeholders* par vos propres informations.

```
aws s3tables put-table-bucket-encryption \
    --table-bucket-arn arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-table-bucket; \
    --encryption-configuration '{
        "sseAlgorithm": "aws:kms",
        "kmsKeyArn": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
    }' \
    --region us-east-1
```

Vous pouvez supprimer le paramètre de chiffrement par défaut pour un bucket de table à l'aide de l'opération DeleteTableBucketEncryptiond'API. Lorsque vous supprimez les paramètres de chiffrement, les nouvelles tables créées dans le compartiment de tables utilisent le chiffrement SSE-S3 par défaut.

Spécification du chiffrement pour les tables

Vous pouvez appliquer le chiffrement SSE-KMS à une nouvelle table lorsque vous la créez à l'aide de moteurs de requêtes, d'opérations d'API REST et du AWS Command Line Interface ()AWS CLI. AWS SDKs Les paramètres de chiffrement que vous spécifiez lors de la création d'une table ont priorité sur le paramètre de chiffrement par défaut du compartiment de table.

> **Note**
>
> Lorsque vous utilisez le chiffrement SSE-KMS pour une table, la clé que vous utilisez pour le chiffrement doit autoriser le principal du service de maintenance des tables S3 à y accéder. Si le directeur du service de maintenance n'y a pas accès, vous ne pourrez pas créer la table.

Pour de plus amples informations, veuillez consulter Octroi des autorisations principales au service de maintenance S3 Tables sur votre clé KMS .

Autorisations nécessaires

Les autorisations suivantes sont requises pour créer des tables chiffrées

- `s3tables:CreateTable`
- `s3tables:PutTableEncryption`

En utilisant le AWS CLI

L' AWS CLI exemple suivant crée une nouvelle table avec un schéma de base et la chiffre à l'aide d'une AWS KMS clé gérée par le client. Pour utiliser la commande, remplacez-la *`user input placeholders`* par vos propres informations.

```
aws s3tables create-table \
  --table-bucket-arn "arn:aws:s3tables:Region:ownerAccountId:bucket/amzn-s3-demo-table-bucket" \
  --namespace "mydataset" \
  --name "orders" \
  --format "ICEBERG" \
  --encryption-configuration '{
    "sseAlgorithm": "aws:kms",
    "kmsKeyArn":
 "arn:aws:kms:Region:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }' \
  --metadata '{
    "iceberg": {
      "schema": {
        "fields": [
          {
            "name": "order_id",
            "type": "string",
            "required": true
          },
          {
            "name": "order_date",
            "type": "timestamp",
            "required": true
```

```
        },
        {
          "name": "total_amount",
          "type": "decimal(10,2)",
          "required": true
        }
      ]
    }
  }
}'
```

La protection des données fait référence à la protection des données lorsqu'elles sont en transit (lorsqu'elles sont acheminées vers et depuis Amazon S3) et au repos (lorsqu'elles sont stockées sur des disques dans les centres de données Amazon S3). S3 Tables protège toujours les données en transit en utilisant Transport Layer Security (1.2 et versions ultérieures) via HTTPS. Pour protéger les données au repos dans des compartiments de table S3, vous disposez des options suivantes :

Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

Le chiffrement est configuré par défaut pour tous les compartiments de table Amazon S3. L'option par défaut pour le chiffrement côté serveur est avec des clés gérées Amazon S3 (SSE-S3). Ce chiffrement est gratuit pour vous et s'applique à toutes les tables de vos compartiments de tables S3, sauf si vous spécifiez une autre forme de chiffrement. Chaque objet est chiffré à l'aide d'une clé unique. Comme protection supplémentaire, SSE-S3 chiffre la clé elle-même à l'aide d'une clé racine dont il effectue une rotation régulière. SSE-S3 utilise l'un des chiffrements par bloc les plus puissants qui existent, Advanced Encryption Standard 256 bits (AES-256), pour chiffrer vos données.

Chiffrement côté serveur avec AWS KMS clés (SSE-KMS)

Vous pouvez choisir de configurer des compartiments de tables ou des tables pour utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Les contrôles de sécurité intégrés AWS KMS peuvent vous aider à respecter les exigences de conformité liées au chiffrement. SSE-KMS vous permet de mieux contrôler vos clés de chiffrement en vous permettant d'effectuer les opérations suivantes :

- Créez, affichez, modifiez, surveillez, activez ou désactivez, faites pivoter et planifiez la suppression des clés KMS.
- Définir les politiques qui contrôlent comment et par qui les clés KMS peuvent être utilisées.
- Suivez l'utilisation des clés AWS CloudTrail pour vérifier que vos clés KMS sont utilisées correctement.

S3 Tables prend en charge l'utilisation de clés gérées par le client dans SSE-KMS pour chiffrer les tables. AWS les clés gérées ne sont pas prises en charge. Pour plus d'informations sur l'utilisation de SSE-KMS pour les tables S3 et les compartiments de tables, consultez. Utilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de tables

Gestion des accès pour S3 Tables

Dans S3 Tables, les ressources incluent les compartiments de tables et les tables qu'ils contiennent. L'utilisateur root du compte Compte AWS qui a créé la ressource (le propriétaire de la ressource) et les utilisateurs AWS Identity and Access Management (IAM) de ce compte qui disposent des autorisations nécessaires peuvent accéder à une ressource qu'ils ont créée. Le propriétaire de la ressource spécifie les autres personnes qui peuvent accéder à la ressource et les actions qu'elles sont autorisées à effectuer sur la ressource. Amazon S3 dispose de différents outils de gestion des accès que vous pouvez utiliser pour accorder à d'autres personnes l'accès à vos ressources S3. Les rubriques suivantes fournissent une vue d'ensemble des ressources, des actions IAM et des clés de condition pour S3 Tables. Elles fournissent également des exemples de politiques basées sur les ressources et basées sur l'identité pour S3 Tables.

Rubriques

- Ressources
- Actions pour S3 Tables
- Clés de condition pour S3 Tables
- Politiques basées sur l'identité IAM pour S3 Tables
- Politiques basées sur les ressources pour S3 Tables
- AWS politiques gérées pour les tables S3
- Octroi d'un accès par le biais de la sémantique SQL

Ressources

Les ressources S3 Tables incluent des compartiments de tables et les tables qu'ils contiennent.

- Compartiments de tables : les compartiments de tables sont spécialement conçus pour les tables et offrent un plus grand nombre de transactions par seconde (TPS) et un meilleur débit de requêtes par rapport aux tables autogérées dans des compartiments S3 à usage général. Les compartiments de tables offrent les mêmes caractéristiques de durabilité, de disponibilité,

de capacité de mise à l'échelle et de performance que les compartiments Amazon S3 à usage général.

- Tables : les tables figurant dans vos compartiments de tables sont stockées au format Apache Iceberg. Vous pouvez interroger ces tables avec du code SQL standard dans des moteurs de requête qui prennent en charge Iceberg.

Amazon Resource Names (ARNs) pour les tables et les compartiments de tables contient l'`s3tables`espace de noms Région AWS, l' Compte AWS ID et le nom du compartiment. Pour accéder à vos tables et compartiments de tables et y effectuer des actions, vous devez utiliser les formats d'ARN suivants :

- Format d'ARN des tables :

  `arn:aws:s3tables:`*`us-west-2`*`:`*`111122223333`*`:bucket/`*`amzn-s3-demo-bucket`*`/table/`*`demo-tableID`*

Actions pour S3 Tables

Dans une politique basée sur l'identité ou sur les ressources, vous définissez quelles actions S3 Tables sont autorisées ou refusées pour des principaux IAM spécifiques. Les actions de tables correspondent à des opérations d'API au niveau du compartiment et de la table. Toutes les actions font partie d'un espace de noms IAM unique : `s3tables`.

Lorsque vous utilisez une action dans une politique, vous autorisez ou refusez généralement l'accès à l'opération d'API du même nom. Toutefois, dans certains cas, une seule action contrôle l'accès à plusieurs opérations d'API. Par exemple, les actions `s3tables:GetTableData` incluent des autorisations pour les opérations d'API `GetObject`, `ListParts` et `ListMultiparts`.

Vous trouverez ci-dessous les actions prises en charge pour les compartiments de tables. Vous pouvez spécifier les actions suivantes dans l'`Action`élément d'une stratégie IAM ou d'une politique de ressources.

Action	Description	Niveau d'accès	Accès intercomptes
`s3tables:CreateTableBucket`	Accorde l'autorisation de créer un	`Write`	Non

Action	Description	Niveau d'accès	Accès intercomptes
	nouveau compartiment		
`s3tables:GetTableBucket`	Accorde l'autorisation de récupérer l'ARN d'un compartiment de tables, le nom du compartiment de tables et sa date de création.	`Write`	Oui
`s3tables:ListTableBuckets`	Accorde l'autorisation de répertorier tous les compartiments de tables du compte.	`Read`	Non
`s3tables:CreateNamespace`	Accorde l'autorisation de créer un espace de noms dans un compartiment de tables	`Write`	Oui

Action	Description	Niveau d'accès	Accès intercomptes
`s3tables:GetNamespace`	Accorde l'autorisation de récupérer les détails de l'espace de noms	`Read`	Oui
`s3tables:ListNamespaces`	Accorde l'autorisation de répertorier tous les espaces de noms figurant dans le compartiment de tables	`Read`	Oui
`s3tables:DeleteNamespace`	Accorde l'autorisation de supprimer un espace de noms dans un compartiment de tables	`Write`	Oui
`s3tables:DeleteTableBucket`	Accorde l'autorisation de supprimer le compartiment	`Write`	Oui

Action	Description	Niveau d'accès	Accès intercomptes
s3tables:PutTableBucketPolicy	Accorde l'autorisation d'ajouter ou de remplacer une politique de compartiment	Permissions Management	Non
s3tables:GetTableBucketPolicy	Accorde l'autorisation de récupérer la politique du compartiment	Read	Non
s3tables:DeleteTableBucketPolicy	Accorde l'autorisation de supprimer la politique de compartiment	Permissions Management	Non
s3tables:GetTableBucketMaintenanceConfiguration	Accorde l'autorisation de récupérer la configuration de maintenance pour un bucket de tables	Read	Oui

Action	Description	Niveau d'accès	Accès intercomptes
`s3tables:PutTableBucketMaintenanceConfiguration`	Accorde l'autorisation d'ajouter ou de remplacer la configuration de la maintenance d'un compartiment de tables	`Write`	Oui
`s3tables:PutTableBucketEncryption`	Accorde l'autorisation d'ajouter ou de remplacer la configuration de chiffrement pour un bucket de tables	`Write`	Non
`s3tables:GetTableBucketEncryption`	Accorde l'autorisation de récupérer la configuration de chiffrement pour un bucket de table	`Read`	Non

Action	Description	Niveau d'accès	Accès intercomptes
`s3tables:DeleteTableBucketEncryption`	Accorde l'autorisation de supprimer la configuration de chiffrement pour un bucket de table	`Write`	Non

Les actions suivantes sont prises en charge pour les tables :

Action	Description	Niveau d'accès	Accès intercomptes
`s3tables:GetTableMaintenanceConfiguration`	Accorde l'autorisation de récupérer la configuration de maintenance d'une table	`Read`	Oui
`s3tables:PutTableMaintenanceConfiguration`	Accorde l'autorisation d'ajouter ou de remplacer la configuration de la maintenance d'une table	`Write`	Oui
`s3tables:PutTablePolicy`	Accorde l'autorisation d'ajouter ou de remplacer	`Permissions Management`	Non

Action	Description	Niveau d'accès	Accès intercomptes
	une politique de table		
`s3tables:GetTablePolicy`	Accorde l'autorisation de récupérer la politique de table	`Read`	Non
`s3tables:DeleteTablePolicy`	Accorde l'autorisation de supprimer la politique de table	`Permissions management`	Non
`s3tables:CreateTable`	Accorde l'autorisation de créer une table dans un compartiment de tables	`Write`	Oui
`s3tables:GetTable`	Accorde l'autorisation de récupérer les informations d'une table.	`Read`	Oui

Action	Description	Niveau d'accès	Accès intercomptes
`s3tables:GetTableMetadataLocation`	Accorde l'autorisation de récupérer le pointeur racine de la table (fichier de métadonnées)	`Read`	Oui
`s3tables:ListTables`	Accorde l'autorisation de répertorier toutes les tables figurant dans un compartiment de tables	`Read`	Oui
`s3tables:RenameTable`	Accorde l'autorisation de modifier le nom d'une table	`Write`	Oui
`s3tables:UpdateTableMetadataLocation`	Accorde l'autorisation de mettre à jour le pointeur racine de la table (fichier de métadonnées)	`Write`	Oui

Action	Description	Niveau d'accès	Accès intercomptes
`s3tables:GetTableData`	Accorde l'autorisation de lire les métadonnées de la table et les objets de données stockés dans le compartiment de tables	`Read`	Oui
`s3tables:PutTableData`	Accorde l'autorisation d'écrire les métadonnées de la table et les objets de données stockés dans le compartiment de tables	`Write`	Oui
`s3tables:GetTableEncryption`	Accorde l'autorisation de récupérer les paramètres de chiffrement d'une table	`Write`	Non
`s3tables:PutTableEncryption`	Accorde l'autorisation d'ajouter du chiffrement à une table	`Write`	Non

Pour effectuer des actions de lecture et d'écriture au niveau des tables, S3 Tables prend en charge les opérations d'API Amazon S3 telles que `GetObject` et `PutObject`. Le tableau suivant fournit la liste des actions au niveau des objets. Lorsque vous accordez des autorisations de lecture et d'écriture à vos tables, vous utilisez les actions suivantes.

Action	Objet S3 APIs
`s3tables:GetTableData`	`GetObject`, `ListParts`, `HeadObject`
`s3tables:PutTableData`	`PutObject`, `CreateMultipartUpload`, `CompleteMultipartUpload`, `UploadPart`, `AbortMultipartUpload`

Par exemple, si un utilisateur dispose d'autorisations `GetTableData`, il peut lire tous les fichiers associés à la table, tels que son fichier de métadonnées, son manifeste, ses fichiers de liste manifeste et ses fichiers de données Parquet.

Clés de condition pour S3 Tables

S3 Tables prend en charge les clés de contexte de condition globales AWS.

S3 Tables définit également les clés de condition suivantes, que vous pouvez utiliser dans une stratégie d'accès.

Clé de condition	Description	Type	
`s3tables:tableName`	Filtre l'accès en fonction du nom des tables dans le compartiment de tables. Vous pouvez utiliser la clé de `s3tables:tableName` condition pour écrire des politiques IAM ou des politiques de compartiment de tables qui limitent l'accès des utilisateurs ou des applications aux seules tables répondant à cette condition de nom. Il est important	`String`	

Clé de condition	Description	Type	
	de noter que si vous utilisez la clé de condition `s3tables:tableName` pour contrôler l'accès, les modifications du nom des tables peuvent avoir un impact sur ces politiques. Exemple de valeur : `"s3tables:tableName":"department*"`		

Clé de condition	Description	Type	
`s3tables:namespace`	Filtre l'accès en fonction des espaces de noms créés dans le compartiment de tables. Vous pouvez utiliser la clé de condition `s3tables:namespace` pour écrire des politiques IAM, de table ou de compartiment de tables qui limitent l'accès des utilisateurs ou des applications aux tables figurant dans un espace de noms spécifique. Exemple de valeur : `"s3tables:namespace":"hr"`	`String`	

Clé de condition	Description	Type	
	Il est important de noter que si vous utilisez la clé de condition `s3tables:namespace` pour contrôler l'accès, les modifications apportées dans les espaces de noms peuvent avoir un impact sur ces politiques.		

Clé de condition	Description	Type	
`s3tables:SSEAlgorithm`	Filtre l'accès par l'algorithme de chiffrement côté serveur utilisé pour chiffrer une table. Vous pouvez utiliser la clé de `s3tables:SSEAlgorithm` condition pour écrire des politiques IAM, de table ou de compartiment de tables qui limitent l'accès des utilisateurs ou des applications aux tables chiffrées avec un certain type de chiffrement. Exemple de valeur : `"s3tables`	`String`	

Clé de condition	Description	Type	
	`:SSEAlgorithm":"aws:kms"` Il est important de noter que si vous utilisez la clé de `s3tables:SSEAlgorithm` condition pour contrôler l'accès, les modifications apportées au chiffrement peuvent avoir un impact sur ces politiques.		

Clé de condition	Description	Type	
`s3tables:KMSKeyArn`	Filtre l'accès par la AWS KMS clé ARN pour la clé utilisée pour chiffrer une table Vous pouvez utiliser la clé de `s3tables:KMSKeyArn` condition pour écrire des politiques IAM, de table ou de compartiment de tables qui limitent l'accès des utilisateurs ou des applications aux tables chiffrées avec une clé KMS spécifique. Il est important de noter que si vous utilisez la clé de	`ARN`	

Clé de condition	Description	Type	
	`s3tables:KMSKeyArn` condition pour contrôler l'accès, la modification de votre clé KMS peut avoir un impact sur ces politiques.		

Politiques basées sur l'identité IAM pour S3 Tables

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ni modifier les tables et les compartiments de tables. Ils ne peuvent pas non plus effectuer de tâches à l'aide de la console s3 AWS Command Line Interface (AWS CLI) ou d'Amazon S3 REST APIs. Pour créer des compartiments de tables et des tables et y accéder, un administrateur AWS Identity and Access Management (IAM) doit accorder les autorisations nécessaires au rôle ou aux utilisateurs 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 dans l'onglet JSON dans le Guide de l'utilisateur IAM.

La rubrique suivante présente des exemples de politiques basées sur l'identité IAM. Pour utiliser les exemples de politiques suivants, remplacez-les *`user input placeholders`* par vos propres informations.

Rubriques

- Exemple 1 : autoriser l'accès pour créer et utiliser des compartiments de tables
- Exemple 2 : autoriser l'accès pour créer et utiliser des tables dans un compartiment de tables

Exemple 1 : autoriser l'accès pour créer et utiliser des compartiments de tables

.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowBucketActions",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTableBucket",
                "s3tables:PutTableBucketPolicy",
                "s3tables:GetTableBucketPolicy",
                "s3tables:ListTableBuckets",
                "s3tables:GetTableBucket"
            ],
            "Resource": "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
        }
    ]
}
```

Exemple 2 : autoriser l'accès pour créer et utiliser des tables dans un compartiment de tables

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowBucketActions",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTable",
                "s3tables:PutTableData",
                "s3tables:GetTableData",
                "s3tables:GetTableMetadataLocation",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:GetNamespace",
                "s3tables:CreateNamespace"
            ],
            "Resource": [
```

```
                "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket",
                "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket/table/*"
            ]
        }
    ]
}
```

Politiques basées sur les ressources pour S3 Tables

S3 Tables fournit des politiques basées sur les ressources pour gérer l'accès aux tables et compartiments de tables : politiques de compartiments de tables et politiques de tables. Vous pouvez utiliser une politique de compartiment de tables pour accorder des autorisations d'accès à l'API au niveau du compartiment de tables, de l'espace de noms ou de la table. Les autorisations attachées au compartiment de tables peuvent s'appliquer à toutes les tables du compartiment ou à des tables spécifiques du compartiment, selon la définition de la politique. Vous pouvez utiliser une politique de tables pour accorder des autorisations au niveau de la table.

Lorsque le service S3 Tables reçoit une demande, il commence par vérifier que le demandeur possède les autorisations nécessaires. Il évalue toutes les stratégies d'accès pertinentes, les politiques utilisateur et les politiques basées sur les ressources pour décider d'autoriser ou non la demande (politique utilisateur IAM, politique de rôle IAM, politique de compartiment de tables et politique de tables). Par exemple, si une politique de compartiment de tables accorde à un utilisateur les autorisations d'effectuer toutes les actions sur les tables du compartiment (y compris `DeleteTable`), mais qu'une table individuelle possède une politique de tables qui refuse l'action `DeleteTable` pour tous les utilisateurs, l'utilisateur ne peut pas supprimer la table.

La rubrique suivante contient des exemples de politiques de tables et de compartiments de tables. Pour utiliser ces politiques, remplacez les *`user input placeholders`* par vos propres informations.

> **Note**
>
> - Chaque politique qui accorde des autorisations pour modifier des tables doit inclure des autorisations pour `GetTableMetadataLocation` afin d'accéder au fichier racine de la table. Pour de plus amples informations, veuillez consulter `GetTableMetadataLocation`.

- Chaque fois que vous effectuez une activité d'écriture ou de suppression sur votre table, incluez les autorisations `UpdateTableMetadataLocation` dans votre stratégie d'accès.
- Nous recommandons d'utiliser une politique de compartiment de tables pour régir l'accès aux actions au niveau du compartiment et une politique de tables pour régir l'accès aux actions au niveau de la table. Dans les cas où vous souhaitez définir le même ensemble d'autorisations sur plusieurs tables, nous vous recommandons d'utiliser une politique de compartiment de tables.

Rubriques

- Exemple 1 : politique de compartiment de tables autorisant l'accès à PutBucketMaintenanceConfiguration pour les compartiments d'un compte
- Exemple 2 : politique de compartiment de tables autorisant l'accès en lecture (SELECT) aux tables stockées dans l'espace de hr noms
- Exemple 3 : politique de tables autorisant l'utilisateur à supprimer une table

Exemple 1 : politique de compartiment de tables autorisant l'accès à **`PutBucketMaintenanceConfiguration`** pour les compartiments d'un compte

L'exemple de politique de compartiment de tables suivant autorise le `data steward` IAM à supprimer les objets non référencés pour tous les compartiments d'un compte en autorisant l'accès à `PutBucketMaintenanceConfiguration`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/datasteward"
            },
            "Action": [
                "s3tables:PutTableBucketMaintenanceConfiguration"
            ],
            "Resource": "arn:aws:s3tables:us-east-1:111122223333:bucket/*"
```

```
        }
    ]
}
```

Exemple 2 : politique de compartiment de tables autorisant l'accès en lecture (SELECT) aux tables stockées dans l'espace de **`hr`** noms

Voici un exemple de politique de compartiment de table qui permet à Jane, une utilisatrice de Compte AWS ID, d'accéder `123456789012` aux tables stockées dans l'espace de `hr` noms d'un compartiment de tables.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Jane"
            },
            "Action": [
                "s3tables:GetTableData",
                "s3tables:GetTableMetadataLocation"
            ],
            "Resource": "arn:aws:s3tables:us-east-1:account_id:bucket/amzn-s3-
demo-table-bucket/table/*",
            "Condition": {
                "StringLike": {
                    "s3tables:namespace": "hr"
                }
            }
        }
    ]
}
```

Exemple 3 : politique de tables autorisant l'utilisateur à supprimer une table

L'exemple suivant de politique de tables autorise le rôle IAM `data steward` à supprimer une table.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "DeleteTable",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/datasteward"
            },
            "Action": [
                "s3tables:DeleteTable",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:PutTableData",
                "s3tables:GetTableMetadataLocation"
            ],
            "Resource": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-
demo-bucket/table/tableUUID"
        }
    ]
}
```

AWS politiques gérées pour les tables S3

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 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.

AWS politique gérée : AmazonS3TablesFullAccess

Vous pouvez associer la politique `AmazonS3TablesFullAccess` à vos identités IAM. Cette politique accorde des autorisations qui permettent un accès complet à Amazon S3 Tables.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3tables:*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AmazonS3TablesReadOnlyAccess

Vous pouvez associer la politique `AmazonS3TablesReadOnlyAccess` à vos identités IAM. Cette politique accorde des autorisations qui permettent d'accéder en lecture seule à Amazon S3 Tables.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3tables:Get*",
```

```
                "s3tables:List*"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politique gérée : AmazonS3TablesLakeFormationServiceRole

Vous pouvez associer la politique `AmazonS3TablesLakeFormationServiceRole` à vos identités IAM. Cette politique accorde des autorisations permettant au rôle AWS Lake Formation de service d'accéder aux tables S3. AWS KMS les autorisations sont utilisées pour permettre à Lake Formation d'accéder aux tables chiffrées.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PermissionsForS3ListTableBuckets",
            "Effect": "Allow",
            "Action": [
                "s3tables:ListTableBuckets"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "DataAccessPermissionsForS3TablesResources",
            "Effect": "Allow",
            "Action": [
                "s3tables:CreateTableBucket",
                "s3tables:GetTableBucket",
```

```
                "s3tables:CreateNamespace",
                "s3tables:GetNamespace",
                "s3tables:ListNamespaces",
                "s3tables:DeleteNamespace",
                "s3tables:DeleteTableBucket",
                "s3tables:CreateTable",
                "s3tables:DeleteTable",
                "s3tables:GetTable",
                "s3tables:ListTables",
                "s3tables:RenameTable",
                "s3tables:UpdateTableMetadataLocation",
                "s3tables:GetTableMetadataLocation",
                "s3tables:GetTableData",
                "s3tables:PutTableData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        },
        {
            "Sid": "KMSDataAccessPermissionsForS3TablesResources",
            "Effect": "Allow",
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "s3.*.amazonaws.com"
                    ],
                    "kms:EncryptionContext:aws:s3:arn":
"arn:aws:s3tables:*:*:bucket/*/table/*"
                },
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
```

```
        },
        {
            "Sid": "KMSDescribeKeyAccessPermissionsForS3TablesResources",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "kms:ViaService": [
                        "s3tables.*.amazonaws.com"
                    ]
                },
                "StringEquals": {
                    "aws:ResourceAccount": "111122223333"
                }
            }
        }
    ]
}
```

Mises à jour Amazon S3 Tables des politiques gérées par AWS

Consultez les détails des mises à jour des politiques AWS gérées pour Amazon S3 Tables depuis que S3 Tables a commencé à suivre ces modifications.

Modification	Description	Date
Amazon S3 Tables a ajouté `AmazonS3TablesLakeFormationServiceRole` .	S3 Tables a ajouté une nouvelle politique AWS gérée appelée`AmazonS3TablesLakeFormationServiceRole` . Cette politique accorde des autorisations qui permettent au rôle de service Lake Formation d'accéder aux tables S3.	19 mai 2025

Modification	Description	Date
Amazon S3 Tables a ajouté `AmazonS3TablesFullAccess` .	S3 Tables a ajouté une nouvelle politique AWS gérée appelée`AmazonS3TablesFullAccess` . Cette politique accorde des autorisations qui permettent un accès complet à Amazon S3 Tables.	3 décembre 2024
Amazon S3 Tables a ajouté `AmazonS3TablesReadOnlyAccess` .	S3 Tables a ajouté une nouvelle politique AWS gérée appelée`AmazonS3TablesReadOnlyAccess` . Cette politique accorde des autorisations qui permettent d'accéder en lecture seule à Amazon S3 Tables.	3 décembre 2024
Amazon S3 Tables a commencé à assurer le suivi des modifications.	Amazon S3 Tables a commencé à suivre les modifications apportées AWS à ses politiques gérées.	3 décembre 2024

Octroi d'un accès par le biais de la sémantique SQL

Vous pouvez accorder des autorisations aux tables en utilisant la sémantique SQL dans les politiques relatives aux tables et aux compartiments de tables. Voici des exemples de sémantique SQL que vous pouvez utiliser :`CREATE`, `INSERT` `DELETE``UPDATE`, et. `ALTER` Le tableau suivant fournit une liste des actions d'API associées à la sémantique SQL que vous pouvez utiliser pour accorder des autorisations à vos utilisateurs.

S3 Tables prend partiellement en charge les autorisations utilisant la sémantique SQL. Par exemple, l'API `CreateTable` crée uniquement une table vide dans le compartiment de tables. Vous avez besoin d'autorisations supplémentaires, telles que `UpdateTableMetadata`, `PutTableData` et `GetTableMetadataLocation`, pour pouvoir définir le schéma de table. Ces autorisations supplémentaires signifient également que vous autorisez également l'utilisateur à insérer des lignes

dans la table. Si vous souhaitez régir l'accès uniquement sur la base de la sémantique SQL, nous vous recommandons d'utiliser AWS Lake Formation ou une solution tierce intégrée avec S3 Tables.

Activité au niveau des tables	Actions IAM		
SELECT	s3tables:GetTableData , s3tables:GetTableMetadataLocation		
CREATE	s3tables:CreateTable , s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation ,		
INSERT	s3tables:UpdateTableMetadataLocation , s3tables:PutTableD		

Activité au niveau des tables	Actions IAM		
	ata , s3tables: GetTableM etadataLo cation		
UPDATE	s3tables: UpdateTab leMetadat aLocation , s3tables: PutTableD ata , s3tables: GetTableM etadataLo cation		
ALTER,RENAME	s3tables: UpdateTab leMetadat aLocation , s3tables: PutTableD ata , s3tables: GetTableM etadataLo cation , s3tables: RenameTab le		

Activité au niveau des tables	Actions IAM		
DELETE,DROP	s3tables:DeleteTable , s3tables:UpdateTableMetadataLocation , s3tables:PutTableData , s3tables:GetTableMetadataLocation		

Connectivité VPC pour les tables S3

Toutes les tables figurant dans S3 Tables sont au format Apache Iceberg et sont composées de deux types d'objets S3. Ces deux types d'objets sont des fichiers de données qui stockent les fichiers de données et de métadonnées qui effectuent le suivi des informations relatives aux fichiers de données à différents points dans le temps. Toutes les opérations relatives aux compartiments de tables, aux espaces de noms et aux tables (par exemple, `CreateNamespace`, `CreateTable`, etc.) sont routées via un point de terminaison S3 Tables (`s3tables.region.amazonaws.com`) et toutes les opérations au niveau des objets qui lisent ou écrivent les fichiers de données et de métadonnées continuent d'être routées via un point de terminaison de service S3 (`s3.region.amazonaws.com`).

Pour accéder aux tables S3, Amazon S3 prend en charge deux types de points de terminaison VPC en utilisant AWS PrivateLink : les points de terminaison de passerelle et les points de terminaison d'interface. Un point de terminaison de passerelle est une passerelle que vous spécifiez dans votre table de routage pour accéder à S3 depuis votre VPC via le AWS réseau. Les points de terminaison d'interface étendent les fonctionnalités des points de terminaison de passerelle en utilisant des

adresses IP privées pour acheminer les demandes vers Amazon S3 depuis votre VPC, sur site, ou depuis un VPC dans un autre en utilisant Région AWS le peering VPC ou. AWS Transit Gateway

Pour accéder à S3 Tables depuis un VPC, nous vous recommandons de créer deux points de terminaison de VPC (un pour S3 et l'autre pour S3 Tables). Vous pouvez créer une passerelle ou un point de terminaison d'interface pour router les opérations de niveau fichier (objet) vers S3 et un point de terminaison d'interface pour router les opérations de niveau compartiment ou table vers S3 Tables. Vous pouvez créer et utiliser des points de terminaison de VPC pour les demandes de niveau fichier à l'aide de S3. Pour plus d'informations, consultez la section Points de terminaison Gateway dans le Guide de AWS PrivateLinkl'utilisateur.

Pour en savoir plus sur la création et l'utilisation AWS PrivateLink de points de terminaison pour les tables S3, consultez les rubriques suivantes. Pour créer un point de terminaison d'interface de VPC, consultez Création d'un point de terminaison de VPC dans le Guide AWS PrivateLink .

Rubriques

- Création de points de terminaison de VPC pour S3 Tables
- Accès aux compartiments de tables et aux tables par le biais de points de terminaison à l'aide du AWS CLI
- Configuration d'un réseau VPC lors de l'utilisation de moteurs de requête
- Restriction de l'accès à S3 Tables au sein du réseau VPC

Création de points de terminaison de VPC pour S3 Tables

Lorsque vous créez un point de terminaison de VPC, S3 Tables génère deux types de noms DNS spécifiques au point de terminaison : régional et zonal.

- Un nom DNS régional a le format suivant : `VPCendpointID.s3tables.AWSregion.vpce.amazonaws.com`. Par exemple, pour l'ID de point de terminaison de VPC `vpce-1a2b3c4d`, le nom DNS généré sera similaire à `vpce-1a2b3c4d-5e6f.s3tables.us-east-1.vpce.amazonaws.com`.
- Un nom DNS zonal a le format suivant : `VPCendpointID-AvailabilityZone.s3tables.AWSregion.vpce.amazonaws.com`. Par exemple, pour l'ID de point de terminaison de VPC `vpce-1a2b3c4d-5e6f.`, le nom DNS généré sera similaire à `vpce-1a2b3c4d-5e6f-us-east-1a.s3tables.us-east-1.vpce.amazonaws.com`.

Un nom DNS zonal inclut votre zone de disponibilité. Vous pouvez utiliser des noms DNS zonaux si votre architecture isole les zones de disponibilité. Les noms DNS S3 spécifiques au point de terminaison peuvent être résolus depuis le domaine DNS public S3.

Vous pouvez également utiliser les options de DNS privé pour simplifier le routage du trafic S3 vers les points de terminaison de VPC et tirer parti du chemin réseau le plus économique disponible pour votre application. Le réseau DNS privé mappe le point de terminaison public de S3 Tables, par exemple `s3tables.region.amazonaws.com`, à une adresse IP privée dans votre VPC. Vous pouvez utiliser les options de DNS privé pour router le trafic S3 régional sans mettre à jour vos clients S3 pour utiliser les noms DNS spécifiques aux points de terminaison de vos points de terminaison d'interface.

> **Note**
>
> AWS PrivateLink pour Amazon S3 ne prend pas en charge l'utilisation de points de terminaison à double pile Amazon S3. Pour plus d'informations, consultez Utilisation des points de terminaison à double pile Amazon S3 dans la Référence d'API Amazon S3.

Accès aux compartiments de tables et aux tables par le biais de points de terminaison à l'aide du AWS CLI

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) pour accéder aux compartiments de tables et aux tables via les points de terminaison de l'interface. Avec les `aws s3` commandes AWS CLI, acheminez le trafic via le point de terminaison Amazon S3. Les `aws s3tables` AWS CLI commandes utilisent le point de terminaison Amazon S3 Tables.

`vpce-0123456afghjipljw-nmopsqea.s3tables.region.vpce.amazonaws.com` est un exemple de point de terminaison de VPC `s3tables`

Un point de terminaison de VPC `s3tables` n'inclut pas de nom de compartiment. Vous pouvez accéder au point de terminaison `s3tables` VPC à l'aide des `aws s3tables` AWS CLI commandes.

`amzn-s3-demo-bucket.vpce-0123456afghjipljw-nmopsqea.s3.region.vpce.amazonaws.com` est un exemple de point de terminaison de VPC `s3`

Vous pouvez accéder au point de terminaison `s3` VPC à l'aide des `aws s3` AWS CLI commandes.

À l'aide du AWS CLI

Pour accéder aux compartiments de tables et aux tables via les points de terminaison de l'interface à l'aide des paramètres AWS CLI, utilisez les paramètres `-region` - et`--endpoint-url`. Pour effectuer des actions de niveau compartiment ou table, utilisez l'URL du point de terminaison S3 Tables. Pour effectuer des actions de niveau objet, utilisez l'URL du point de terminaison Amazon S3.

Dans les exemples suivants, remplacez le *`user input placeholders`* par vos propres informations.

Exemple 1 : utilisation d'une URL de point de terminaison pour répertorier les compartiments de tables dans votre compte

```
aws s3tables list-table-buckets --endpoint https://vpce-0123456afghjipljb-
aac.s3tables.us-east-1.vpce.amazonaws.com –region us-east-1
```

Exemple 2 : utilisation d'une URL de point de terminaison pour répertorier les tables dans votre compartiment

```
aws s3tables list-tables --table-bucket-arn arn:aws:s3tables:us-
east-1:123456789301:bucket/amzn-s3-demo-bucket --endpoint
 https://vpce-0123456afghjipljb-aac.s3tables.us-east-1.vpce.amazonaws.com --region us-
east-1
```

Configuration d'un réseau VPC lors de l'utilisation de moteurs de requête

Effectuez les étapes suivantes pour configurer un réseau VPC lorsque vous utilisez des moteurs de requête.

1. Pour commencer, vous pouvez créer ou mettre à jour un VPC. Pour plus d'informations, consultez Création d'un VPC.
2. Pour les opérations de niveau table ou compartiment de tables qui sont routées vers S3 Tables, créez un nouveau point de terminaison d'interface. Pour plus d'informations, consultez Accéder à un AWS service à l'aide d'un point de terminaison VPC d'interface.
3. Pour toutes les opérations de niveau objet qui sont routées vers Amazon S3, créez un point de terminaison de passerelle ou un point de terminaison d'interface. Pour plus d'informations sur les points de terminaison de passerelle, consultez Création d'un point de terminaison de passerelle.
4. Configurez ensuite vos ressources de données et lancez un cluster Amazon EMR. Pour plus d'informations, consultez Démarrer avec Amazon EMR.

5. Vous pouvez ensuite soumettre une application Spark avec une configuration supplémentaire en sélectionnant vos noms DNS depuis le point de terminaison de VPC. Par exemple, `spark.sql.catalog.ice_catalog.s3tables.endpoint` et `https://interface-endpoint.s3tables.us-east-1.vpce.amazonaws.com`. Pour plus d'informations, consultez Soumettre un travail à votre cluster Amazon EMR.

Restriction de l'accès à S3 Tables au sein du réseau VPC

Comme pour les politiques basées sur les ressources, vous pouvez attacher une politique de points de terminaison à votre point de terminaison de VPC qui contrôle l'accès aux tables et aux compartiments de tables. Dans l'exemple suivant, la politique de point de terminaison d'interface restreint l'accès à des compartiments de tables spécifiques uniquement.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "Policy141511512309",
    "Statement": [
        {
            "Sid": "Access-to-specific-bucket-only",
            "Principal": "*",
            "Action": "s3tables:*",
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket",
                "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

Considérations et restrictions de sécurité pour S3 Tables

La liste suivante décrit les caractéristiques et les fonctionnalités de sécurité et de contrôle d'accès qui ne sont pas prises en charge ou qui sont restreintes pour S3 Tables.

- Les stratégies d'accès public ne sont pas prises en charge. Les utilisateurs ne peuvent pas modifier les politiques de compartiments ou de tables pour autoriser l'accès public.
- Les objets présignés URLs pour accéder aux objets associés à une table ne sont pas pris en charge.
- Les balises ne sont pas prises en charge pour les tables et les compartiments de tables. En conséquence, la prise en charge du contrôle d'accès basé sur les attributs et de l'allocation basée sur les balises n'est pas disponible.
- Les demandes effectuées via HTTP ne sont pas prises en charge. Amazon S3 répond automatiquement par une redirection HTTP pour toutes les demandes effectuées via HTTP afin de les mettre à niveau vers HTTPS.
- Vous devez utiliser AWS la version 4 de Signature lorsque vous envoyez des demandes à un point d'accès à l'aide du REST APIs.
- Les requêtes effectuées via le protocole Internet version 6 (IPv6) ne sont prises en charge que pour les actions au niveau des objets sur les points de terminaison de stockage des tables, et non pour les actions au niveau des tables et des compartiments.
- Les stratégies d'accès des tables et des compartiments de tables sont limitées à une taille de 20 Ko.

Journalisation avec AWS CloudTrail pour les tables S3

Amazon S3 est intégré à AWS 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 Amazon S3 sous forme d'événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon S3, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires. Lorsqu'une activité événementielle prise en charge se produit dans Amazon S3, cette activité est enregistrée dans un CloudTrail événement. Vous pouvez utiliser le journal AWS CloudTrail pour consigner les événements de gestion et les événements de données pour les tables S3. Pour plus d'informations, consultez les sections CloudTrail Événements Amazon S3 et Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail événements de gestion pour les tables S3

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre AWS compte.

Par défaut, CloudTrail enregistre les événements de gestion pour les tables S3. Les événements CloudTrail de gestion `eventsource` pour les tables S3 sont `s3tables.amazonaws.com`. Lorsque vous configurez votre AWS compte, les événements CloudTrail de gestion sont activés par défaut. Les événements de gestion suivants sont enregistrés CloudTrail.

- CreateNamespace
- CreateTable
- CreateTableBucket
- DeleteNamespace
- DeleteTable
- DeleteTableBucket
- DeleteTableBucketPolicy
- DeleteTablePolicy
- GetNamespace
- GetTable
- GetTableBucket
- GetTableBucketMaintenanceConfiguration
- GetTableBucketPolicy
- GetTableMaintenanceConfiguration
- GetTableMaintenanceJobStatus
- GetTableMetadataLocation
- GetTablePolicy
- ListNamespaces
- ListTableBuckets
- ListTables
- PutTableBucketMaintenanceConfiguration
- PutTableMaintenanceConfiguration
- PutBucketPolicy
- PutTablePolicy
- RenameTable

- `UpdateTableMetadataLocation`

Pour plus d'informations sur les événements CloudTrail de gestion, consultez la section Journalisation des événements de gestion dans le Guide de AWS CloudTrail l'utilisateur.

CloudTrail événements de données pour les tables S3

Les événements de données fournissent des informations sur les opérations de ressources effectuées sur ou dans une ressource. Par défaut, les CloudTrail traces n'enregistrent pas les événements de données, mais vous pouvez configurer les pistes pour enregistrer les événements de données.

Lorsque vous enregistrez des événements de données pour un trail in CloudTrail, vous choisissez ou spécifiez le type de ressource. S3 Tables possède deux types de ressources, `AWS::S3Tables::Table` et `AWS::S3Tables::TableBucket`.

Les événements de données suivants sont enregistrés CloudTrail.

- `AbortMultipartUpload`
- `CompleteMultipartUpload`
- `CreateMultipartUpload`
- `GetObject`
- `HeadObject`
- `ListParts`
- `PutObject`
- `UploadPart`

Pour plus d'informations sur les événements CloudTrail liés aux données, consultez la section Enregistrement des événements liés aux données dans le Guide de AWS CloudTrail l'utilisateur.

Pour plus d'informations sur les CloudTrail événements relatifs aux tables S3, consultez les rubriques suivantes :

Rubriques

- AWS CloudTrail exemples de fichiers journaux d'événements de données pour les tables S3

AWS CloudTrail exemples de fichiers journaux d'événements de données pour les tables S3

Un fichier AWS CloudTrail journal contient des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. Cette rubrique fournit des exemples de fichiers journaux pour les événements de CloudTrail données relatifs aux tables S3.

Rubriques

- Exemple : fichier CloudTrail journal d'un événement GetObject de données
- Exemple : fichier CloudTrail journal d'un événement PutObject de données

Exemple : fichier CloudTrail journal d'un événement **`GetObject`** de données

L'exemple suivant montre un exemple de fichier CloudTrail journal qui illustre le fonctionnement de l'`GetObject`API.


```
{
    "eventVersion": "1.11",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "123456789012",
      "arn": "arn:aws:iam::111122223333:user/"myUserName",
      "accountId": "111122223333",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName":"myUserName"
    },
    "eventTime": "2024-11-22T17:12:25Z",
    "eventSource": "s3tables.amazonaws.com",
    "eventName": "GetObject",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "[aws-cli/2.18.5]",
    "requestParameters": {
        "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
        "key": "product-info.json"
    },
    "responseElements":  null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
```

```
            "bytesTransferredIn": 0,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhNJYmhg",
            "bytesTransferredOut": 28441

          },
          "requestID": "07D681123BD12AED",
          "eventID": "f2b287f3-0df1-1234-a2f4-c4bdfed47657",
          "readOnly": true,
          "resources": [{
              "accountId": "111122223333",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "111122223333",
              "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:111122223333:bucket/amzn-s3-demo-
bucket/table/111aa1111-22bb-33cc-44dd-5555eee66ffff"

           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
           "recipientAccountId": "444455556666",
           "eventCategory": "Data",
           "tlsDetails": {
             "tlsVersion": "TLSv1.2",
             "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
             "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
          }
    }
```

Exemple : fichier CloudTrail journal d'un événement **PutObject** de données

L'exemple suivant montre un exemple de fichier CloudTrail journal qui illustre le fonctionnement de l'PutObjectAPI.

```
{
        "eventVersion": "1.11",
        "userIdentity": {
          "type": "IAMUser",
          "principalId": "123456789012",
```

```
          "arn":  "arn:aws:iam::444455556666:user/"myUserName",
          "accountId": "444455556666",
          "accessKeyId": "AKIAI44QH8DHBEXAMPLE",
          "userName":"myUserName"
        },
        "eventTime": "2024-11-22T17:12:25Z",
        "eventSource": "s3tables.amazonaws.com",
        "eventName": "PutObject",
        "awsRegion": "us-east-1",
        "sourceIPAddress": "192.0.2.0",
        "userAgent": "[aws-cli/2.18.5]",
        "requestParameters": {
            "Host": "tableWarehouseLocation.s3.us-east-1.amazonaws.com",
            "key": "product-info.json"
        },
        "responseElements":  {
            "x-amz-server-side-encryption": "AES256",
            "x-amz-version-id": "13zAFMdccAjt3MWd6ehxgCCCDRdkAKDw"
        },
        "additionalEventData": {
            "SignatureVersion": "SigV4",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "bytesTransferredIn": 28441,
            "AuthenticationMethod": "AuthHeader",
            "xAmzId2": "q6xhCJYmhg",
            "bytesTransferredOut": 0

          },
          "requestID": "28d2faaf-1234-4649-997d-EXAMPLE72818",
          "eventID": "694d604a-d190-1234-0dd1-EXAMPLEe20c1",
          "readOnly": false,
          "resources": [{
              "accountId": "444455556666",
              "type": "AWS::S3Tables::TableBucket",
               "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1"
           }, {
              "accountId": "444455556666",
              "type": "AWS::S3Tables::Table",
              "ARN": "arn:aws:s3tables:us-east-1:444455556666:bucket/amzn-s3-demo-
bucket1/table/b89ec883-b1d9-4b37-9cd7-b86f590123f4"
           }],
           "eventType": "AwsApiCall",
           "managementEvent": false,
```

```
            "recipientAccountId": "111122223333",
            "eventCategory": "Data",
            "tlsDetails": {
              "tlsVersion": "TLSv1.2",
              "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
              "clientProvidedHostHeader": "tableWarehouseLocation.s3.us-
east-1.amazonaws.com"
             }
          }
```

Utilisation de vecteurs S3 et de buckets vectoriels

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Qu'est-ce qu'Amazon S3 Vectors ?

Amazon S3 Vectors fournit un stockage vectoriel spécialement conçu et optimisé en termes de coûts pour vos applications de recherche sémantique et d'intelligence artificielle. Grâce à l'élasticité et à la durabilité d'Amazon S3 permettant de stocker des ensembles de données vectorielles avec des performances de requête inférieures à une seconde, S3 Vectors est idéal pour les applications qui ont besoin de créer et de développer des index vectoriels. Vous bénéficiez d'un ensemble dédié d'opérations d'API pour stocker, accéder et exécuter des requêtes de similarité sur des données vectorielles sans provisionner d'infrastructure. S3 Vectors se compose de plusieurs composants clés qui fonctionnent ensemble :

- Buckets vectoriels : nouveau type de compartiment spécialement conçu pour stocker et interroger des vecteurs.
- Index vectoriels : dans un compartiment vectoriel, vous pouvez organiser vos données vectorielles dans des index vectoriels. Vous effectuez des requêtes de similarité sur vos données vectorielles au sein d'index vectoriels.
- Vecteurs — Vous stockez des vecteurs dans votre index vectoriel. Pour les applications de recherche de similarité et d'intelligence artificielle, les vecteurs sont créés sous forme d'intégrations vectorielles, qui sont des représentations numériques qui préservent les relations sémantiques entre les contenus (tels que le texte, les images ou le son) afin que les éléments similaires soient placés plus près les uns des autres. Les vecteurs S3 peuvent effectuer des recherches de similarité basées sur le sens sémantique plutôt que sur une correspondance exacte en comparant mathématiquement la proximité des vecteurs les uns aux autres. Lorsque vous ajoutez des données vectorielles à un index vectoriel, vous pouvez également joindre des métadonnées pour les futures requêtes de filtrage en fonction d'un ensemble de conditions (par exemple, les horodatages, les catégories et les préférences de l'utilisateur).

Les écritures dans les vecteurs S3 sont très cohérentes, ce qui signifie que vous pouvez accéder immédiatement aux dernières données ajoutées. Au fur et à mesure que vous écrivez, mettez à jour et supprimez des vecteurs, S3 Vectors optimise automatiquement les données vectorielles afin d'obtenir le meilleur rapport qualité-prix possible pour le stockage vectoriel, même lorsque les ensembles de données sont mis à l'échelle et évoluent. Vous pouvez contrôler l'accès à vos données vectorielles à l'aide des mécanismes de contrôle d'accès existants d'Amazon S3, notamment les politiques relatives aux compartiments et à l'IAM. Pour plus d'informations sur les limites d'index vectoriel par compartiment et les limites vectorielles par indice, consultezLimites et restrictions.

Cas d'utilisation : recherches de similarité dans de grands ensembles de données

Les recherches de similarité vous permettent de trouver des éléments conceptuellement liés les uns aux autres en fonction de leurs représentations vectorielles, plutôt que de leurs correspondances exactes par mots clés. Ces recherches permettent d'identifier des contenus ayant des significations ou des caractéristiques similaires, même lorsque les mots exacts ou les éléments visuels diffèrent.

Les cas d'utilisation courants de la recherche de similarité avec les vecteurs S3 incluent :

- Imagerie médicale - Trouvez des similitudes entre des millions d'images médicales pour faciliter le diagnostic et la planification du traitement
- Violation du droit d'auteur - Identifiez le contenu potentiellement dérivé dans les grandes médiathèques
- Déduplication d'images : détectez et supprimez les images dupliquées ou quasi-dupliquées dans de grandes collections d'images
- Compréhension vidéo : recherchez des scènes ou du contenu spécifiques dans des ressources vidéo
- Recherche de documents d'entreprise - Activez la recherche sémantique dans les documents d'entreprise pour trouver des informations pertinentes en fonction du sens
- Personnalisation - Fournissez des recommandations personnalisées en recherchant des articles similaires

Vous devez utiliser S3 Vectors si vous souhaitez créer des applications rentables de recherche vectorielle et d'intelligence artificielle avec des temps de recherche inférieurs à la seconde. Avec les compartiments vectoriels, vous ne payez que pour ce que vous utilisez et vous pouvez réduire les

coûts liés au téléchargement, au stockage et à l'interrogation des intégrations vectorielles. Pour plus d'informations sur la tarification, consultez Tarification Amazon S3.

Caractéristiques des vecteurs S3

Stockage spécialement conçu pour les vecteurs

S3 Vectors est le premier système de stockage d'objets spécialement conçu dans le cloud pour stocker et interroger des vecteurs. Les compartiments vectoriels sont conçus pour fournir un stockage rentable, élastique et durable pour les données vectorielles.

Les intégrations vectorielles transforment la façon dont les clients utilisent et extraient leurs données non structurées, qu'il s'agisse de détecter des similitudes entre des images médicales, de détecter des anomalies dans des milliers d'heures de séquences vidéo, de naviguer dans de grandes bases de code ou d'identifier la jurisprudence la plus pertinente pour une question juridique donnée. Ces applications émergentes se combinent à des modèles d'intégration pour encoder la signification sémantique des données (par exemple, texte, images, vidéo, code) sous forme d'intégrations vectorielles numériques.

Dans un bucket vectoriel, vous organisez vos données vectorielles au sein d'index vectoriels, sans infrastructure de provisionnement. Au fur et à mesure que vous écrivez, mettez à jour et supprimez des vecteurs, les vecteurs S3 optimisent automatiquement les données vectorielles afin d'obtenir le meilleur rapport qualité-prix possible pour le stockage vectoriel, même lorsque les ensembles de données sont mis à l'échelle et évoluent. Pour plus d'informations sur les limites d'index vectoriel par compartiment et les limites vectorielles par indice, consultezLimites et restrictions.

Réaliser des requêtes de similarité

Avec S3 Vectors, vous pouvez effectuer des requêtes de similarité efficaces pour trouver les vecteurs les plus similaires à un vecteur de requête, avec des temps de réponse inférieurs à la seconde. S3 Vectors est idéal pour les charges de travail où les requêtes sont moins fréquentes.

Filtrage des métadonnées

Vous pouvez joindre des métadonnées (par exemple, année, auteur, genre et lieu) sous forme de paires clé-valeur à vos vecteurs. Par défaut, toutes les métadonnées sont filtrables, sauf si vous les spécifiez explicitement comme non filtrables. Vous pouvez utiliser des métadonnées filtrables pour filtrer les résultats de vos requêtes en fonction d'attributs spécifiques, afin d'améliorer la pertinence

de vos requêtes. Les index vectoriels prennent en charge les types de métadonnées de type chaîne, numérique, booléen et liste. Pour plus d'informations sur les limites de taille des métadonnées par vecteur et les limites de taille des métadonnées filtrables par vecteur, consultezLimites et restrictions.

Gestion des accès et sécurité

Vous pouvez gérer l'accès aux ressources dans des compartiments vectoriels à l'aide des politiques IAM et de contrôle des services dans AWS Organizations. S3 Vectors utilise un espace de noms de service différent de celui d'Amazon S3 : l'espace de `s3vectors` noms. Par conséquent, vous pouvez concevoir des politiques spécifiques pour le service S3 Vectors et ses ressources. Vous pouvez concevoir des politiques pour autoriser l'accès à des index vectoriels individuels, à tous les index vectoriels d'un compartiment vectoriel ou à tous les compartiments vectoriels d'un compte. Tous les paramètres d'accès public par blocs d'Amazon S3 sont toujours activés pour les compartiments vectoriels et ne peuvent pas être désactivés.

Intégration aux AWS services

S3 Vectors s'intègre à d'autres AWS services pour améliorer vos capacités de traitement vectoriel :

- Amazon OpenSearch Service - Optimisez les coûts de stockage vectoriel tout en continuant à utiliser les opérations OpenSearch d'API. C'est la solution idéale pour les charges de travail qui nécessitent des fonctionnalités de recherche avancées telles que la recherche hybride, les agrégations, le filtrage avancé et la recherche à facettes. Vous pouvez également exporter un instantané d'un index vectoriel S3 vers Amazon OpenSearch Serverless pour une recherche vectorielle à QPS élevé et à faible latence.
- Bases de connaissances Amazon Bedrock - Sélectionnez un index vectoriel dans S3 Vectors comme magasin de vecteurs afin d'économiser sur les coûts de stockage pour les applications de génération augmentée (RAG) par extraction.
- Amazon Bedrock dans SageMaker Unified Studio - Développez et testez des bases de connaissances en utilisant S3 Vectors comme magasin de vecteurs.

Tutoriel : Débuter avec les vecteurs S3

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Dans ce didacticiel, vous allez créer un compartiment vectoriel S3 et un index vectoriel Région AWS dans la console Amazon S3. Ensuite, vous utilisez un modèle d'intégration Amazon Bedrock pour générer des intégrations vectorielles de vos données et les stocker dans votre index vectoriel pour effectuer des recherches sémantiques.

Pour commencer, créez un AWS compte si vous n'en avez pas déjà un. Pour plus d'informations sur la configuration d'un compte, consultezPremiers pas avec Amazon S3.

Rubriques

- Étape 1 : créer un bucket vectoriel avec la console
- Étape 2 : créer un index vectoriel dans un bucket vectoriel avec la console
- Étape 3 : Insérer des vecteurs dans un index vectoriel avec le SDK pour Python (SDK for Python)
- Étape 4 : Vecteurs de requête dans un index vectoriel avec le SDK pour Python (Boto3)
- (Facultatif) Automatisez la création d'intégrations vectorielles avec la CLI S3 Vectors Embed
- (Facultatif) Intégrez les vecteurs S3 aux bases de connaissances Amazon Bedrock
- (Facultatif) Intégrez les vecteurs S3 à Amazon OpenSearch

Étape 1 : créer un bucket vectoriel avec la console

Les compartiments vectoriels S3 sont un type de compartiment Amazon S3 spécialement conçu pour stocker et interroger des vecteurs. Vous utilisez des opérations d'API dédiées pour écrire et interroger des données vectorielles. Vous pouvez contrôler l'accès à vos données vectorielles à l'aide de mécanismes de contrôle d'accès tels que les politiques basées sur l'identité IAM et les politiques basées sur les ressources.

Au cours de cette étape, vous utilisez la console Amazon S3 pour créer votre premier compartiment vectoriel. Pour d'autres méthodes de création d'un compartiment vectoriel, consultezCréation d'un bucket vectoriel.

Pour créer un bucket vectoriel

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Vector buckets.
3. Sur la page Compartiments vectoriels, choisissez Créer un compartiment vectoriel.

4. Sur la page Créer un compartiment vectoriel, dans le champ Nom du compartiment vectoriel, entrez un nom. Dans ce didacticiel, nous utilisons *media-embeddings* comme nom de compartiment vectoriel. Les noms de compartiments vectoriels doivent comporter de 3 à 63 caractères et être uniques au sein d'un Région AWS. Les caractères valides sont les lettres minuscules (a-z), les chiffres (0-9) et les traits d'union (-).

   > **Note**
   >
   > Le nom du bucket vectoriel ne peut pas être modifié une fois le bucket créé.

5. Sous Chiffrement, choisissez Spécifier le type de cryptage. Vous avez la possibilité de spécifier le type de chiffrement : chiffrement côté serveur avec AWS Key Management Service clés (SSE-KMS) ou chiffrement côté serveur par défaut avec clés gérées Amazon S3 (SSE-S3). Dans ce didacticiel, nous avons choisi le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Pour plus d'informations sur la définition de la configuration de chiffrement pour les compartiments vectoriels, consultezProtection des données et chiffrement dans S3 Vectors.

   > **Note**
   >
   > Le type de chiffrement ne peut pas être modifié une fois le bucket vectoriel créé.

6. Choisissez Create vector bucket.

Étape 2 : créer un index vectoriel dans un bucket vectoriel avec la console

> **Note**
>
> Choisissez soigneusement les paramètres de configuration de votre index vectoriel. Après avoir créé un index vectoriel, vous ne pouvez pas mettre à jour le nom de l'index vectoriel, la dimension, la métrique de distance ou les clés de métadonnées non filtrables. Pour modifier l'une de ces valeurs, vous devez créer un nouvel index vectoriel.

Au cours de cette étape, vous allez créer un index vectoriel dans votre compartiment vectoriel. L'index vectoriel est utilisé pour stocker et interroger vos intégrations vectorielles. Pour plus d'informations sur les index vectoriels, consultezIndices vectoriels.

Pour créer un index vectoriel

1. Accédez au compartiment vectoriel nouvellement créé dans la liste des compartiments vectoriels de la console Amazon S3.
2. Choisissez Créer un index vectoriel.
3. Sur la page Créer un index vectoriel, entrez un nom dans le champ Nom de l'index vectoriel. Dans ce didacticiel, nous utilisons *movies* comme nom d'index vectoriel.

   Les noms des index vectoriels doivent comporter de 3 à 63 caractères et être uniques dans ce compartiment vectoriel. Les caractères valides sont les lettres minuscules (a-z), les chiffres (0-9), les traits d'union (-) et les points (.).

   Le nom de l'index vectoriel ne peut pas être modifié après la création de l'index.
4. Sous Dimension, spécifiez une valeur numérique comprise entre 1 et 4096 qui détermine le nombre de nombres contenus dans chaque vecteur généré par votre modèle d'intégration de vecteurs. Les modèles d'intégration sont des modèles d'apprentissage automatique (ML) spécialisés qui convertissent des données (telles que du texte ou des images) en vecteurs numériques. Les modèles d'intégration produisent généralement des sorties comprises entre 500 et 2 000 dimensions, chaque dimension étant un nombre à virgule flottante. Dans ce didacticiel, nous utiliserons le modèle d'intégration Titan Text v2 d'Amazon Bedrock. Ce modèle d'intégration utilise des vecteurs à 1024 dimensions par défaut. Nous allons donc définir la dimension de l'indice vectoriel sur. `1024`

   La valeur de dimension ne peut pas être modifiée après la création de l'index. Spécifiez soigneusement la valeur de dimension en fonction des recommandations de votre modèle d'intégration.
5. Sous Métrique de distance, choisissez Cosinus (qui mesure la similarité angulaire) ou Euclidean (qui mesure la distance en ligne droite) comme métrique de distance pour définir le mode de calcul de la similitude entre les vecteurs lors des requêtes. Dans ce tutoriel, nous avons choisi Cosine.

   La métrique de distance ne peut pas être modifiée après la création de l'index. Choisissez soigneusement la métrique de distance en fonction des recommandations de votre modèle d'intégration.
6. Sous Paramètres supplémentaires (facultatif), vous pouvez spécifier des clés de métadonnées non filtrables pour stocker des informations supplémentaires à côté de vos intégrations vectorielles.

> **Note**
>
> Vous pouvez associer des métadonnées filtrables sous forme de paires clé-valeur à chaque vecteur lorsque vous insérez des données vectorielles après la création de l'index. Par défaut, toutes les clés de métadonnées associées aux vecteurs sont filtrables et peuvent être utilisées comme filtres dans une requête de similarité. Seules les clés de métadonnées spécifiées comme non filtrables lors de la création de l'index vectoriel sont exclues du filtrage.

Chaque clé de métadonnées non filtrable doit comporter entre 1 et 63 caractères et être unique dans l'index vectoriel. Ces clés sont utiles pour stocker des informations de référence que vous n'avez pas besoin de filtrer lors des requêtes de similarité. Par exemple, lorsque vous travaillez avec des intégrations de texte, vous souhaiterez peut-être conserver les fragments de texte d'origine à des fins de référence. Dans ce didacticiel, nous ajoutons une clé de métadonnées non filtrable nommée `source_text` pour stocker les données de texte pour lesquelles nous voulons créer des intégrations vectorielles.

Vous ne pouvez pas mettre à jour les clés de métadonnées non filtrables après la création de l'index. Planifiez soigneusement votre structure de métadonnées.

7. Choisissez Créer un index vectoriel.

Vérifiez que votre nouvel index vectoriel apparaît dans le compartiment.

Étape 3 : Insérer des vecteurs dans un index vectoriel avec le SDK pour Python (SDK for Python)

Pour insérer, répertorier et interroger des vecteurs, utilisez l' AWS SDKsAPI REST AWS CLI, ou Amazon S3.

Cette étape consiste à insérer des intégrations vectorielles dans votre index vectoriel à l'aide de l'PutVectorsopération API.

Vous devez d'abord générer des intégrations vectorielles en utilisant le modèle d'intégration de votre choix. Si vous utilisez Amazon Bedrock, générez des intégrations en utilisant l'opération d'InvokeModelAPI pour spécifier votre modèle d'intégration préféré. Vous pouvez également générer

et insérer des intégrations vectorielles à l'aide d'une seule commande, voir. (Facultatif) Automatisez la création d'intégrations vectorielles avec la CLI S3 Vectors Embed

L'exemple de code suivant génère des intégrations vectorielles à 1024 dimensions avec le modèle Titan Text Embeddings V2 d'Amazon Bedrock en utilisant AWS SDK pour Python (Boto3) le, et les stocke dans votre index vectoriel à l'aide de l'API. `PutVectors` À chaque vecteur, nous associons des paires clé-valeur sous forme de métadonnées filtrables. De plus, nous utilisons une clé de métadonnées non filtrable dont le nom *`source_text`* permet de préserver le texte original dont chaque vecteur est dérivé. Pour optimiser le débit des demandes et optimiser la vitesse et l'efficacité, nous vous recommandons d'insérer et de supprimer des vecteurs par lots. Pour de plus amples informations, veuillez consulter Meilleures pratiques en matière de vecteurs S3.

```
# Populate a vector index with embeddings from Amazon Titan Text Embeddings V2.
import boto3
import json

# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Texts to convert to embeddings.
texts = [
    "Star Wars: A farm boy joins rebels to fight an evil empire in space",
    "Jurassic Park: Scientists create dinosaurs in a theme park that goes wrong",
    "Finding Nemo: A father fish searches the ocean to find his lost son"
]

# Generate vector embeddings.
embeddings = []
for text in texts:
    response = bedrock.invoke_model(
        modelId="amazon.titan-embed-text-v2:0",
        body=json.dumps({"inputText": text})
    )

    # Extract embedding from response.
    response_body = json.loads(response["body"].read())
    embeddings.append(response_body["embedding"])

# Write embeddings into vector index with metadata.
s3vectors.put_vectors(
    vectorBucketName="media-embeddings",
```

```
    indexName="movies",
    vectors=[
        {
            "key": "Star Wars",
            "data": {"float32": embeddings[0]},
            "metadata": {"source_text": texts[0], "genre":"scifi"}
        },
        {
            "key": "Jurassic Park",
            "data": {"float32": embeddings[1]},
            "metadata": {"source_text": texts[1], "genre":"scifi"}
        },
        {
            "key": "Finding Nemo",
            "data": {"float32": embeddings[2]},
            "metadata": {"source_text": texts[2], "genre":"family"}
        }
    ]
)
```

Étape 4 : Vecteurs de requête dans un index vectoriel avec le SDK pour Python (Boto3)

Après avoir enregistré les intégrations de vos vecteurs dans l'index vectoriel, vous pouvez effectuer une recherche de similarité à l'aide de l'QueryVectorsopération API.

Vous devez d'abord générer vos intégrations vectorielles de requête en utilisant le même modèle d'intégration que celui utilisé lors de l'insertion dans. Étape 3 : Insérer des vecteurs dans un index vectoriel avec le SDK pour Python (SDK for Python) Dans ce didacticiel, utilisez le modèle Titan Text Embeddings V2 d'Amazon Bedrock via le SDK pour Python (Boto3).

Vous pouvez effectuer une recherche de similarité pour obtenir les vecteurs correspondants les plus proches. Dans une recherche de similarité, vous pouvez éventuellement filtrer à l'aide de clés de métadonnées pour affiner les résultats en fonction de critères spécifiques tout en préservant la pertinence sémantique.

```
# Query a vector index with an embedding from Amazon Titan Text Embeddings V2.
import boto3
import json

# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
```

```
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Query text to convert to an embedding.
input_text = "adventures in space"

# Generate the vector embedding.
response = bedrock.invoke_model(
    modelId="amazon.titan-embed-text-v2:0",
    body=json.dumps({"inputText": input_text})
)

# Extract embedding from response.
model_response = json.loads(response["body"].read())
embedding = model_response["embedding"]

# Query vector index.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    returnDistance=True,
    returnMetadata=True
)
print(json.dumps(response["vectors"], indent=2))

# Query vector index with a metadata filter.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    filter={"genre": "scifi"},
    returnDistance=True,
    returnMetadata=True
)
print(json.dumps(response["vectors"], indent=2))
```

(Facultatif) Automatisez la création d'intégrations vectorielles avec la CLI S3 Vectors Embed

Amazon S3 Vectors Embed CLI est un outil de ligne de commande autonome qui simplifie le processus d'utilisation des intégrations vectorielles dans les vecteurs S3. À l'aide de commandes uniques, vous pouvez créer des intégrations vectorielles pour vos données à l'aide d'Amazon Bedrock, puis les stocker et les interroger dans votre index vectoriel S3. L'outil prend en charge les commandes suivantes :

- `s3vectors-embed put`: générez des intégrations vectorielles de texte, de contenu de fichier ou d'objets S3, et stockez-les sous forme de vecteurs dans un index vectoriel S3.
- `s3vectors-embed query`: Incorporez une entrée de requête et recherchez des vecteurs similaires dans un index vectoriel S3.

Pour plus d'informations sur les commandes et leur utilisation, consultez le GitHub référentiel Amazon S3 Vectors Embed CLI.

(Facultatif) Intégrez les vecteurs S3 aux bases de connaissances Amazon Bedrock

Les bases de connaissances Amazon Bedrock s'intègrent aux vecteurs S3 pour un stockage rentable et à long terme des ensembles de données vectorielles.

Prérequis

Suivez les prérequis pour vous assurer que vous disposez des autorisations nécessaires pour créer une base de connaissances Amazon Bedrock.

- Autorisations IAM appropriées pour les services S3 Vectors et Amazon Bedrock. Pour plus d'informations sur les autorisations IAM pour les vecteurs S3, consultezGestion des identités et des accès dans S3 Vectors.
- Vos documents sources ont été préparés pour être intégrés à la base de connaissances.
- Compréhension des exigences de votre modèle d'intégration.

Créez une base de connaissances Amazon Bedrock avec des vecteurs S3 dans la console

Les bases de connaissances Amazon Bedrock fournissent un flux de travail end-to-end RAG entièrement géré. Lorsque vous créez une base de connaissances avec S3 Vectors, Amazon Bedrock extrait automatiquement les données de votre source de données S3, convertit le contenu en blocs de texte, génère des intégrations et les stocke dans votre index vectoriel. Vous pouvez ensuite interroger la base de connaissances et générer des réponses basées sur des fragments extraits de vos données sources.

Pour créer une base de connaissances Amazon Bedrock avec des vecteurs S3 dans la console

1. Connectez-vous à l' AWS Management Console aide d'un rôle IAM avec les autorisations Amazon Bedrock et ouvrez la console Amazon Bedrock à l'adresse. https://console.aws.amazon.com/bedrock/
2. Dans le volet de navigation de gauche, sélectionnez Knowledge Bases.
3. Dans la section Bases de connaissances, choisissez Create. Dans la liste déroulante, choisissez Base de connaissances avec magasin vectoriel.
4. Dans ce didacticiel, conservez le nom de la base de connaissances, la description de la base de connaissances et les autorisations IAM à leurs valeurs par défaut.
5. Pour Choisir un type de source de données, choisissez la source de données à laquelle connecter votre base de connaissances. Dans ce didacticiel, choisissez Amazon S3.
6. (Facultatif) Fournissez des balises ou des journaux d'application.
7. Choisissez Suivant.
8. Sur la page Configurer la source de données, conservez les paramètres par défaut du nom de la source de données, de l'emplacement de la source de données, de la stratégie d'analyse et de la stratégie de segmentation dans les paramètres par défaut de ce didacticiel.
9. Dans l'URI S3, entrez le compartiment S3 à usage général qui contient vos fichiers source, ou choisissez Browse S3 et choisissez le compartiment à usage général S3.
10. Pour les données S3 chiffrées, sélectionnez Ajouter une clé KMS gérée par le client pour les données S3 et spécifiez votre clé KMS gérée par le client.
11. Choisissez Next pour passer à l'étape suivante qui spécifie le modèle d'intégration et les options de stockage vectoriel.

12. Dans la section Modèle d'intégration, choisissez Sélectionner le modèle et choisissez un modèle d'intégration compatible avec les vecteurs S3. Vous devez utiliser des intégrations à virgule flottante. Le type binaire n'est pas pris en charge.
13. (Facultatif) Développez la section Configurations supplémentaires pour voir les options de configuration suivantes (tous les modèles ne prennent pas en charge toutes les configurations) :
    - Type d'intégration : s'il faut convertir les données en intégrations vectorielles à virgule flottante (float32) (plus précises, mais plus coûteuses) ou en intégrations vectorielles binaires (moins précises, mais moins coûteuses). Pour intégrer les vecteurs S3, vous devez choisir les intégrations vectorielles à virgule flottante.
    - Dimensions vectorielles : choisissez la taille de dimension recommandée pour les modèles d'intégration.
14. Dans la section Magasin de vecteurs, choisissez la méthode recommandée Création rapide d'un nouveau magasin de vecteurs pour la configuration automatique d'un nouveau compartiment de vecteurs, ou choisissez Utiliser un magasin de vecteurs existant pour utiliser un compartiment de vecteurs existant s'il est disponible. Pour plus d'informations sur l'utilisation d'un flux de magasin vectoriel existant, consultez la section Conditions préalables à l'utilisation d'un magasin vectoriel que vous avez créé pour une base de connaissances dans le guide de l'utilisateur d'Amazon Bedrock.
15. Pour les configurations supplémentaires : par défaut, votre compartiment vectoriel utilise le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Vous pouvez choisir d'utiliser votre propre clé KMS pour le chiffrement côté serveur avec les clés du service de gestion des AWS clés (SSE-KMS) pour un meilleur contrôle des paramètres de chiffrement.
16. Choisissez Suivant pour consulter les détails de la base de connaissances, puis choisissez Créer une base de connaissances.

> **Note**
>
> Le temps nécessaire à la création d'une base de connaissances dépend de vos configurations spécifiques. Lorsque la création d'une base de connaissances est terminée, le statut de la base de connaissances change pour indiquer qu'elle est prête ou disponible. Une fois que votre base de connaissances est prête et disponible, synchronisez votre source de données pour la première fois ou chaque fois que vous souhaitez maintenir votre contenu à jour. Pour synchroniser votre source de données, choisissez votre base de

connaissances dans la console et choisissez Synchroniser dans la section d'aperçu de la source de données.

(Facultatif) Intégrez les vecteurs S3 à Amazon OpenSearch

Amazon OpenSearch Service est un service entièrement géré qui simplifie le déploiement, le dimensionnement et le fonctionnement OpenSearch dans le AWS cloud. Il existe deux intégrations entre S3 Vectors et OpenSearch. La première consiste à exporter des données vectorielles de S3 Vectors vers OpenSearch Serverless pour des capacités de recherche performantes. L'autre utilise S3 Vectors comme moteur de stockage rentable tout OpenSearch en conservant l'accès aux OpenSearch fonctionnalités.

Pour de plus amples informations, veuillez consulter Utilisation de vecteurs S3 avec OpenSearch Service.

Seaux vectoriels

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Les compartiments vectoriels sont un type de compartiment Amazon S3 conçu spécifiquement pour le stockage et l'interrogation de données vectorielles. Les compartiments vectoriels utilisent des outils dédiés APIs pour gérer efficacement les données vectorielles et réduire les coûts de téléchargement, de stockage et d'interrogation des intégrations vectorielles. Les compartiments vectoriels constituent la base de l'organisation de vos données vectorielles en index, ce qui vous permet d'effectuer des recherches de similarité dans de grands ensembles de données tout en bénéficiant de la disponibilité, de la durabilité, de l'évolutivité et de la rentabilité d'Amazon S3.

Les compartiments vectoriels sont optimisés pour le stockage de vecteurs à long terme avec des temps de recherche inférieurs à la seconde. Vous pouvez effectuer des requêtes de similarité sur vos données vectorielles et éventuellement joindre des métadonnées pour filtrer les requêtes en fonction de conditions spécifiques telles que les dates, les catégories ou les préférences de l'utilisateur.

Chaque compartiment vectoriel est associé à un Amazon Resource Name (ARN) unique et à une politique de ressources. Les ARNs compartiments vectoriels suivent le format suivant :

```
arn:aws:s3vector:Region:OwnerAccountID:bucket/bucket-name
```

Dans un bucket vectoriel, vous créez des index vectoriels pour stocker et interroger vos données. Chaque compartiment vectoriel existe dans une AWS région spécifique et vous pouvez créer plusieurs index vectoriels dans un compartiment vectoriel. Les compartiments vectoriels prennent en charge les mécanismes de sécurité et de contrôle d'accès, notamment les politiques basées sur l'identité IAM et les politiques de compartiment. Vous pouvez utiliser des politiques de compartiment pour accorder ou restreindre l'accès à des index spécifiques au sein de votre compartiment vectoriel.

Principales caractéristiques des seaux vectoriels :

- Conçu spécialement pour le stockage vectoriel et les opérations de recherche de similarité.
- Des écritures très cohérentes garantissent que les données vectorielles sont immédiatement accessibles.
- Optimisation automatique des données vectorielles pour un meilleur rapport prix/performances à mesure que les ensembles de données évoluent.

Pour plus d'informations sur les limites d'index vectoriel par compartiment et les autres limitations, consultezLimites et restrictions.

Rubriques

- Règles de dénomination des compartiments vectoriels
- Création d'un bucket vectoriel
- Répertorier les seaux vectoriels
- Affichage des attributs d'un bucket vectoriel
- Supprimer un compartiment vectoriel vide
- Gestion des politiques relatives aux compartiments vectoriels

Règles de dénomination des compartiments vectoriels

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Les noms de compartiments vectoriels doivent respecter des conventions de dénomination spécifiques afin de garantir l'unicité au sein d'une AWS région. Amazon S3 applique les exigences de dénomination des compartiments suivantes, et vous ne pouvez pas créer de compartiment vectoriel si ces règles ne sont pas respectées. En outre, certaines bonnes pratiques, bien qu'elles ne soient pas appliquées, aident à prévenir les conflits lors de l'utilisation de compartiments vectoriels par programmation ou via la console.

Exigences relatives à la dénomination des compartiments vectoriels

Lorsque vous créez des compartiments vectoriels, vous devez respecter les exigences suivantes :

- Les noms de compartiments vectoriels doivent être uniques dans le même AWS compte pour chaque AWS région.
- Les noms des compartiments vectoriels doivent comporter entre 3 et 63 caractères.
- Les noms de compartiments vectoriels ne peuvent être composés que de lettres minuscules (a-z), de chiffres (0-9) et de traits d'union (-).
- Les noms de compartiments vectoriels doivent commencer et se terminer par une lettre ou un chiffre.

Bonnes pratiques en matière de dénomination

Nous vous recommandons de suivre les meilleures pratiques suivantes lorsque vous nommez vos compartiments vectoriels :

- Utilisez des noms descriptifs qui reflètent l'objectif de vos données vectorielles (par exemple, recommandations de produits, incorporations de documents).
- Évitez d'utiliser des informations sensibles dans les noms de compartiments, car elles peuvent apparaître dans les journaux et URLs.

- Veillez à ce que les noms soient concis mais significatifs pour en faciliter la gestion et l'identification.

Ces conventions de dénomination garantissent que vos compartiments vectoriels sont accessibles de manière fiable via la console AWS de gestion, l'API REST Amazon S3, la AWS CLI et AWS SDKs.

Création d'un bucket vectoriel

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez créer un bucket vectoriel à l'aide de la console S3 ou de la AWS CLI. Toutes les données stockées dans des compartiments vectoriels sont toujours cryptées au repos. Par défaut, les compartiments vectoriels utilisent le SSE-S3 pour chiffrer les données vectorielles. Vous pouvez choisir de configurer les buckets pour qu'ils utilisent plutôt le chiffrement côté serveur avec des clés du AWS Key Management Service (AWS KMS) (SSE-KMS). Les paramètres de chiffrement du bucket ne peuvent pas être modifiés après la création d'un bucket vectoriel. Il est donc important de choisir la méthode de chiffrement appropriée en fonction de vos exigences de sécurité et de conformité. Pour plus d'informations sur la sécurité dans les compartiments vectoriels, consultezProtection des données et chiffrement dans S3 Vectors.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Vector buckets.
3. Choisissez Create vector bucket.
4. Pour le nom du compartiment vectoriel, entrez le nom de votre compartiment.

   Le nom du bucket doit respecter les règles de dénomination :

   - Le nom du compartiment doit comporter entre 3 et 63 caractères.
   - Le nom du compartiment ne peut inclure que des lettres minuscules, des chiffres et des traits d'union.

- Le nom du compartiment doit être unique dans votre AWS compte pour une AWS région.

Pour plus d'informations sur les règles de dénomination des compartiments vectoriels, consultezRègles de dénomination des compartiments vectoriels.

> **Important**
>
> Vous ne pouvez pas modifier le nom du bucket vectoriel après l'avoir créé.

5. Pour le chiffrement, choisissez l'une des options suivantes :

- Ne spécifiez pas le type de chiffrement : Amazon S3 applique automatiquement le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de chiffrement de base pour les nouveaux vecteurs. Choisissez cette option pour la configuration la plus simple sans configuration supplémentaire.
- Spécifier le type de cryptage : choisissez une méthode de cryptage spécifique :
  - Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) — Choisissez explicitement d'utiliser SSE-S3. Amazon S3 chiffre vos données vectorielles lorsqu'elles sont enregistrées dans le stockage et les déchiffre lorsque vous y accédez. AWS gère automatiquement toutes les clés de chiffrement.
  - Chiffrement côté serveur avec AWS clés du service de gestion des clés (SSE-KMS) : utilise des clés gérées par le client (CMKs) pour vous permettre AWS KMS de mieux contrôler vos clés de chiffrement, la rotation des clés et les politiques d'accès.

    Si vous sélectionnez SSE-KMS, des options supplémentaires s'offrent à vous :

    - Choisissez parmi vos AWS KMS clés : sélectionnez une clé gérée par le client existante dans votre compte.
    - Entrez l'ARN de la AWS KMS clé : spécifiez l'ARN complet d'une clé KMS (format obligatoire).
    - Créer une clé KMS : ouvre la console AWS KMS pour créer une nouvelle clé gérée par le client.

    Exigences clés du KMS :

    - La clé KMS doit se trouver dans la même région que le compartiment vectoriel.
    - Vous devez spécifier l'ARN complet de la clé KMS (la clé IDs et les alias ne sont pas pris en charge).

- Vous devez autoriser le principal du service S3 Vectors (`indexing.s3vectors.amazonaws.com`) à utiliser la clé. `kms:Decrypt` Pour plus d'informations sur un exemple de politique AWS KMS clé, consultezProtection des données et chiffrement dans S3 Vectors.

Pour des informations détaillées sur les options de chiffrement et la configuration des clés KMS, consultezUtilisation du chiffrement SSE-KMS.

> **Important**
>
> Les paramètres de chiffrement ne peuvent pas être modifiés une fois le bucket vectoriel créé. Choisissez avec soin en fonction de vos exigences de sécurité et de conformité à long terme.

6. Choisissez Create vector bucket.

Après la création, vous verrez un message de confirmation. Le nouveau compartiment vectoriel apparaît dans votre liste de compartiments vectoriels et est prêt à être créé des index vectoriels dans le compartiment.

En utilisant le AWS CLI

Vous pouvez créer un compartiment vectoriel avec chiffrement SSE-S3 à l'aide de la commande suivante. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3vectors create-vector-bucket \
   --vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Pour créer un bucket vectoriel avec chiffrement SSE-KMS à l'aide d'une clé KMS gérée par le client :

```
aws s3vectors create-vector-bucket \
   --vector-bucket-name "amzn-s3-demo-vector-bucket" \
   --encryption-configuration '{"sseType": "aws:kms", "kmsKeyArn": "arn:aws:kms:us-
east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"}'
```

Répertorier les seaux vectoriels

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez consulter tous vos compartiments vectoriels à l'aide de la console Amazon S3 ou du AWS CLI. Les opérations de mise en vente prennent en charge le filtrage basé sur des préfixes pour vous aider à trouver des compartiments spécifiques lorsque votre compte contient de nombreux compartiments vectoriels. Pour plus d'informations sur `ListVectorBuckets` les limites de préfixes et les limites de réponse, consultez le ListVectorBucketsmanuel de référence des API Amazon S3.

Fonctionnalité de recherche de préfixes

La recherche par préfixe vous permet de répertorier les compartiments commençant par un préfixe spécifique, ce qui facilite l'organisation et la recherche de compartiments vectoriels associés. Cela est particulièrement utile lorsque vous utilisez des conventions de dénomination qui regroupent les buckets associés :

- Basé sur l'environnement :`production-vectors-`, `staging-vectors-` `dev-vectors-`
- Basé sur des cas d'utilisation :`ml-model-vectors-`, `document-search-` `image-similarity-`
- Basé sur le travail d'équipe :`data-science-vectors-`, `ml-platform-vectors-`

Utilisation de la console S3

Pour répertorier les buckets vectoriels

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Vector buckets.

   La console affiche la liste de tous vos compartiments vectoriels avec les informations suivantes :

   - Nom — Le nom unique du compartiment vectoriel
   - Date de création : date à laquelle le bucket a été créé

- Amazon Resource Name (ARN) — L'ARN complet pour l'accès programmatique

Pour filtrer la liste :

- Pour rechercher un bucket en fonction du début de son nom, entrez un nom de bucket vectoriel ou un préfixe dans le champ de recherche au-dessus de la liste des bucket.
- Utilisez des préfixes pour rechercher des groupes de compartiments connexes (par exemple, tapez « prod- » pour trouver tous les compartiments de production)

  La liste est mise à jour en temps réel au fur et à mesure que vous tapez

Affichage des attributs d'un bucket vectoriel

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez consulter des informations détaillées sur un bucket vectoriel, notamment ses propriétés, ses paramètres de chiffrement et les détails de création.

Supprimer un compartiment vectoriel vide

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez supprimer un bucket vectoriel lorsque vous n'en avez plus besoin. Pour supprimer un compartiment vectoriel, vous devez d'abord supprimer tous les index vectoriels qu'il contient. Lorsque vous supprimez un index vectoriel, toutes les données vectorielles qu'il contient sont supprimées. Utilisez la AWS CLI ou l'API pour supprimer un bucket ou un index vectoriel. SDKs Vous ne pouvez pas supprimer un bucket vectoriel ou un index vectoriel à l'aide de la console.

Avant de pouvoir supprimer un bucket vectoriel, vous devez :

- Supprimez tous les index vectoriels du compartiment.
- Assurez-vous qu'aucune opération n'est en cours sur le bucket ou ses index.

> **Important**
>
> - La suppression du bucket est définitive et ne peut pas être annulée.
> - Toutes les données et configurations associées au bucket sont définitivement perdues.
> - Le nom du bucket peut être réutilisé après sa suppression.
> - Toutes les applications ou tous les scripts faisant référence au bucket recevront des erreurs après leur suppression.

À l'aide du AWS CLI

Vérifiez d'abord qu'aucun index vectoriel n'existe dans le compartiment. Pour plus d'informations sur la façon de vérifier que le compartiment est vide, consultezRépertorier les index vectoriels.

Si des index existent, vous devez supprimer tous les vecteurs de chaque index, puis supprimer les index. Pour plus d'informations sur la façon de vérifier que le compartiment est vide, reportez-vous aux Supprimer des vecteurs d'un index vectoriel sectionsVecteurs de listes, etSupprimer un index vectoriel.

Pour supprimer le compartiment vectoriel vide, utilisez l'exemple de commande suivant et remplacez-le *`user input placeholders`* par vos propres informations.

```
aws s3vectors delete-vector-bucket \
  --vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Gestion des politiques relatives aux compartiments vectoriels

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Les politiques de compartiment vectoriel sont des politiques basées sur les ressources que vous attachez directement aux compartiments vectoriels pour contrôler l'accès au compartiment et à son contenu. Vous pouvez ajouter, afficher, modifier et supprimer des politiques relatives aux compartiments vectoriels. Les politiques relatives aux compartiments vectoriels peuvent accorder des autorisations aux principaux d'autres AWS comptes, ce qui les rend utiles pour les scénarios d'accès entre comptes.

Opérations de gestion des politiques

- PutVectorBucketPolicy— Ajoutez ou mettez à jour une politique de compartiment.
- GetVectorBucketPolicy— Récupère la politique de compartiment actuelle.
- DeleteVectorBucketPolicy— Supprimez la politique relative aux compartiments.

Ajouter une politique de bucket vectoriel

À l'aide du AWS CLI

Pour ajouter ou mettre à jour une politique de compartiment, utilisez l'exemple de commande suivant et *user input placeholders* remplacez-la par vos propres informations.

```
aws s3vectors put-vector-bucket-policy \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --policy '{"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::111122223333:root"},"Action":"s3vectors:*","Resource":"arn:aws:s3vectors:a
region:111122223333:bucket/amzn-s3-demo-vector-bucket"}]}'
```

Afficher une politique de bucket vectoriel

À l'aide du AWS CLI

Pour récupérer une politique de compartiment, utilisez l'exemple de commande suivant et *user input placeholders* remplacez-la par vos propres informations.

```
aws s3vectors get-vector-bucket-policy \
  --vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Suppression d'une politique de compartiment vectoriel

À l'aide du AWS CLI

Pour supprimer une politique de compartiment, utilisez l'exemple de commande suivant et *`user input placeholders`* remplacez-la par vos propres informations.

```
aws s3vectors delete-vector-bucket-policy \
  --vector-bucket-name "amzn-s3-demo-vector-bucket"
```

Pour obtenir des informations détaillées sur la création et la gestion des politiques de compartiment, notamment des exemples de politiques et les meilleures pratiques, consultezExemples de politiques basées sur les ressources S3 Vectors.

Indices vectoriels

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

> **Note**
>
> Choisissez soigneusement les paramètres de configuration de votre index vectoriel. Après avoir créé un index vectoriel, vous ne pouvez pas mettre à jour le nom de l'index vectoriel, la dimension, la métrique de distance ou les clés de métadonnées non filtrables. Pour modifier l'une de ces valeurs, vous devez créer un nouvel index vectoriel.

Les index vectoriels sont des ressources contenues dans des compartiments vectoriels qui stockent et organisent les données vectorielles pour des opérations de recherche de similarité efficaces. Lorsque vous créez un index vectoriel, vous spécifiez la métrique de distance (`CosineouEuclidean`), le nombre de dimensions qu'un vecteur doit avoir et, éventuellement, une liste de champs de métadonnées que vous souhaitez exclure du filtrage lors des requêtes de similarité.

Pour plus d'informations sur les limites d'index vectoriel par compartiment, les limites vectorielles par index et les limites de dimension par vecteur, consultezLimites et restrictions.

Chaque index vectoriel possède un Amazon Resource Name (ARN) unique. Les ARNs index vectoriels suivent le format suivant :

```
arn:aws:s3vectors:region:account-id:bucket/bucket-name/index/index-name
```

Exigences relatives à la dénomination des index vectoriels

- Les noms des index vectoriels doivent être uniques dans le compartiment vectoriel.
- Les noms des index vectoriels doivent comporter entre 3 et 63 caractères.
- Les caractères valides sont les lettres minuscules (a-z), les chiffres (0-9), les traits d'union (-) et les points (.).
- Les noms des index vectoriels doivent commencer et se terminer par une lettre ou un chiffre.

Exigences relatives aux dimensions

Une dimension est le nombre de valeurs d'un vecteur. Tous les vecteurs ajoutés à l'index doivent avoir exactement ce nombre de valeurs.

- Une dimension doit être un entier compris entre 1 et 4096.
- Une plus grande dimension nécessite plus d'espace de stockage.

Options de mesure de distance

La métrique de distance indique le mode de calcul de la similarité entre les vecteurs. Lorsque vous créez des intégrations vectorielles, choisissez la métrique de distance recommandée pour votre modèle d'intégration pour des résultats plus précis.

- Cosinus — Mesure le cosinus de l'angle entre les vecteurs. Idéal pour les vecteurs normalisés et lorsque la direction compte plus que la magnitude.
- Euclidean — Mesure la distance en ligne droite entre les vecteurs. Il est préférable de le faire lorsque la direction et l'amplitude sont importantes.

Clés de métadonnées non filtrables

Les clés de métadonnées vous permettent d'associer des informations supplémentaires à vos vecteurs sous forme de paires clé-valeur lors du stockage et de la récupération. Par défaut, toutes

les métadonnées sont filtrables. Vous pouvez donc les utiliser pour filtrer les résultats des requêtes. Toutefois, vous pouvez désigner des clés de métadonnées spécifiques comme non filtrables lorsque vous souhaitez stocker des informations à l'aide de vecteurs sans les utiliser pour le filtrage.

Contrairement aux clés de métadonnées par défaut, ces clés ne peuvent pas être utilisées comme filtres de requête. Les clés de métadonnées non filtrables peuvent être récupérées mais ne peuvent pas être recherchées, interrogées ou filtrées. Vous ne pouvez y accéder qu'après avoir trouvé l'index.

Les clés de métadonnées non filtrables vous permettent d'enrichir les vecteurs avec du contexte supplémentaire que vous souhaitez récupérer avec les résultats de recherche sans avoir besoin de filtrer. Un exemple courant de clé de métadonnées non filtrable est lorsque vous incorporez du texte dans des vecteurs et que vous souhaitez inclure le texte original lui-même en tant que métadonnées non filtrables. Cela vous permet de renvoyer le texte source à côté des résultats de recherche vectorielle sans augmenter les limites de taille des métadonnées filtrables. D'autres exemples incluent le stockage des horodatages de création, de la source URLs ou des informations descriptives à des fins de référence uniquement. Les clés de métadonnées non filtrables sont accessibles lors de la récupération de vecteurs mais, contrairement aux clés de métadonnées par défaut, elles ne peuvent pas être utilisées comme filtres de requête.

Les exigences relatives aux clés de métadonnées non filtrables sont les suivantes.

- Les clés de métadonnées non filtrables doivent être uniques dans l'index vectoriel.
- Les clés de métadonnées non filtrables doivent comporter entre 1 et 63 caractères.
- Les clés de métadonnées non filtrables ne peuvent pas être modifiées une fois l'index vectoriel créé.
- Les vecteurs S3 prennent en charge jusqu'à 10 clés de métadonnées non filtrables par index.

Rubriques

- Création d'un index vectoriel dans un compartiment vectoriel
- Répertorier les index vectoriels
- Supprimer un index vectoriel

Création d'un index vectoriel dans un compartiment vectoriel

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

> **Note**
>
> Choisissez soigneusement les paramètres de configuration de votre index vectoriel. Après avoir créé un index vectoriel, vous ne pouvez pas mettre à jour le nom de l'index vectoriel, la dimension, la métrique de distance ou les clés de métadonnées non filtrables. Pour modifier l'une de ces valeurs, vous devez créer un nouvel index vectoriel.

Un index vectoriel est une ressource au sein d'un bucket vectoriel qui stocke et organise les données vectorielles pour une recherche de similarité efficace. Lorsque vous créez un index vectoriel, vous définissez les caractéristiques que tous les vecteurs de cet index doivent partager, telles que la dimension, la métrique de distance utilisée pour les calculs de similarité et, éventuellement, les clés de métadonnées non filtrables. Pour plus d'informations sur les exigences de dénomination des index vectoriels, les exigences en matière de dimensions, les options de mesure de distance et les clés de métadonnées non filtrables, consultez. Limites et restrictions

Les index vectoriels doivent être créés dans un compartiment vectoriel existant et nécessitent des paramètres de configuration spécifiques qui ne peuvent pas être modifiés après leur création.

Utilisation de la console S3

Pour créer un index vectoriel

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Vector buckets.
3. Dans la liste des compartiments vectoriels, choisissez le nom du compartiment dans lequel vous souhaitez créer un index vectoriel.
4. Choisissez Créer un index vectoriel.
5. Dans Nom de l'index vectoriel, entrez le nom de votre index vectoriel.

Les noms des index vectoriels doivent être uniques dans le compartiment vectoriel. Le nom de l'index doit comporter entre 3 et 63 caractères. Les caractères valides sont les lettres minuscules (a-z), les chiffres (0-9), les traits d'union (-) et les points (.). Pour plus d'informations sur les exigences de dénomination des index vectoriels, reportez-vous àLimites et restrictions.

6. Pour Dimension, entrez le nombre de valeurs dans chaque vecteur.

> **Note**
>
> - La valeur de Dimension détermine le nombre de valeurs numériques que chaque vecteur contiendra.
> - Tous les vecteurs ajoutés à cet index doivent avoir exactement ce nombre de valeurs.
> - La dimension doit être comprise entre 1 et 4096.
> - Une plus grande dimension nécessite plus d'espace de stockage.
> - Choisissez en fonction des dimensions de sortie de votre modèle d'intégration.

Pour plus d'informations sur les exigences relatives aux dimensions, consultezLimites et restrictions.

7. Pour la métrique de distance, choisissez l'une des options suivantes :
   - Cosinus — Mesure le cosinus de l'angle entre les vecteurs. Idéal pour les vecteurs normalisés et lorsque la direction compte plus que la magnitude
   - Euclidean — Mesure la distance en ligne droite entre les vecteurs. Il est préférable de le faire lorsque la direction et l'amplitude sont importantes.
8. (Facultatif) Sous Métadonnées non filtrables, configurez les clés de métadonnées qui seront stockées mais non utilisées pour le filtrage :

   Pour ajouter des clés de métadonnées non filtrables :

   a. Sélectionnez Ajouter une clé.

   b. Entrez un nom de clé (1 à 63 caractères et unique dans cet index vectoriel).

   c. Répétez l'opération pour ajouter des clés supplémentaires (10 clés au maximum).

> **Note**
>
> Vous pouvez associer des métadonnées filtrables sous forme de paires clé-valeur à chaque vecteur lorsque vous insérez des données vectorielles après avoir créé un index vectoriel. Par défaut, toutes les clés de métadonnées associées aux vecteurs sont filtrables et peuvent être utilisées comme filtres dans une requête de similarité. Seules les clés de métadonnées spécifiées comme non filtrables lors de la création de l'index vectoriel sont exclues du filtrage. Pour plus d'informations sur les limites de taille des métadonnées par vecteur, y compris les contraintes de métadonnées totales et filtrables, consultezLimites et restrictions.

9. Passez en revue votre configuration avec soin.

> **Note**
>
> Ces paramètres ne peuvent pas être modifiés après leur création.

10. Choisissez Créer un index vectoriel.

À l'aide du AWS CLI

Pour créer un index vectoriel dans un compartiment vectoriel, utilisez les exemples de commandes suivants et remplacez-le `user input placeholders` par vos propres informations.

Exemple 1 : Création d'un index vectoriel avec des clés de métadonnées non filtrables

```
aws s3vectors create-index \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --index-name "idx" \
  --data-type "float32" \
  --dimension 1 \
  --distance-metric "cosine" \
  --metadata-configuration '{"nonFilterableMetadataKeys":["nonFilterableKey1"]}'
```

Exemple 2 : Création d'un index vectoriel sans clés de métadonnées non filtrables

```
aws s3vectors create-index \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --index-name "idx2" \
  --data-type "float32" \
  --dimension 4096 \
  --distance-metric "euclidean"
```

En outre, toutes les métadonnées (filtrables et non filtrables) sont extraites de la même manière à l'aide des opérations de l'API `GetVectors`ListVectors, ou `QueryVectors` de l'API. La commande CLI suivante montre comment récupérer des vecteurs avec des métadonnées (y compris des métadonnées non filtrables).

Exemple de demande :

```
aws s3vectors get-vectors \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --index-name "idx" \
  --keys '["vec1", "vec3"]' \
  --return-data \
  --return-metadata \
```

Exemple de réponse :

```
{
    "vectors": [
        {
            "key": "vec1",
            "data": {
                "float32": [
                    0.10000000149011612,
                    0.20000000298023224,
                    0.30000001192092896,
                    0.4000000059604645,
                    0.5
                ]
            },
            "metadata": {
                "category": "test",
                "text": "First vector"
            }
        },
```

```
        {
            "key": "vec3",
            "data": {
                "float32": [
                    0.6000000238418579,
                    0.699999988079071,
                    0.800000011920929,
                    0.8999999761581421,
                    1.0
                ]
            },
            "metadata": {
                "text": "Third vector",
                "category": "test"
            }
        }
    ]
}
```

La réponse inclura toutes les métadonnées associées au vecteur, qu'il ait été spécifié comme filtrable ou non filtrable lors de la création de l'index.

Répertorier les index vectoriels

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez afficher tous les index vectoriels contenus dans un compartiment vectoriel. L'opération de listage prend en charge le filtrage basé sur les préfixes pour vous aider à trouver des index spécifiques lorsqu'un compartiment contient de nombreux index. Pour plus d'informations sur `ListIndexes` les limites de préfixes et les limites de réponse, consultez le ListIndexesmanuel Amazon Simple Storage Service API Reference.

Fonctionnalité de recherche de préfixes

La recherche par préfixe vous permet de répertorier les index commençant par un préfixe spécifique, ce qui facilite l'organisation et la recherche des index vectoriels associés. Cela est particulièrement utile lorsque vous utilisez des conventions de dénomination qui regroupent des index connexes :

- Par type de données : `text-embeddings-image-features-`, `audio-vectors-`
- Par modèle :`model1-embeddings-`,`model2-vectors-`, `custom-model-`
- Par cas d'utilisation :`search-index-`,`recommendation-`, `similarity-`
- Par environnement :`prod-vectors-`,`staging-vectors-`, `dev-vectors-`

Utilisation de la console S3

Pour répertorier les index vectoriels

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Vector buckets.
3. Dans la liste des compartiments vectoriels, choisissez le nom du compartiment contenant les index que vous souhaitez afficher.
4. La console affiche une liste complète de tous les index vectoriels du compartiment, notamment :
   - Nom : nom de chaque index.
   - Date de création : date de création de l'index.
   - Amazon Resource Name (ARN) : ARN complet pour chaque index.

Pour filtrer la liste

1. Entrez un nom ou un préfixe d'index dans le champ de recherche situé au-dessus de la liste d'index. Utilisez des préfixes pour rechercher des groupes d'index connexes.
2. La liste est mise à jour en temps réel au fur et à mesure que vous tapez.

À l'aide du AWS CLI

Utilisez les exemples de commandes suivants et remplacez-les *`user input placeholders`* par vos propres informations.

Pour répertorier les index dotés d'un préfixe spécifique dans un compartiment vectoriel

Exemple de demande :

```
aws s3vectors list-indexes \
  --vector-bucket-name "amzn-s3-demo-bucket" \
  --prefix "idx" \
  --max-results 1
```

Exemple de réponse :

```
{
    "nextToken":
 "lObb29ZkzxMGtBXs97Rkbs26xdtKemu4brsnq2jX8DCocADkILv5cRphemXS3PXXFnQBihQBmESgEeKaGA",
    "indexes": [
        {
            "vectorBucketName": "amzn-s3-demo-bucket",
            "indexName": "idx",
            "indexArn": "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-
vector-bucket/index/idx",
            "creationTime": "2025-06-12T15:50:23+00:00"
        }
    ]
}
```

Pour répertorier les index avec pagination

Exemple de demande :

```
aws s3vectors list-indexes \
  --vector-bucket-name "amzn-s3-demo-bucket" \
  --prefix "idx" \
  --next-token
 "lObb29ZkzxMGtBXs97Rkbs26xdtKemu4brsnq2jX8DCocADkILv5cRphemXS3PXXFnQBihQBmESgEeKaGA"
```

Exemple de réponse :

```
{
    "indexes": [
        {
            "vectorBucketName": "amzn-s3-demo-bucket",
            "indexName": "idx2",
            "indexArn": "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-
vector-bucket/index/idx2",
            "creationTime": "2025-06-12T15:45:37+00:00"
```

```
        }
    ]
}
```

Supprimer un index vectoriel

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez supprimer un index vectoriel lorsque vous n'en avez plus besoin. Cette opération supprime définitivement l'index et tous les vecteurs qu'il contient.

> **Important**
>
> Lorsque vous supprimez un index vectoriel, vous devez connaître les points suivants :
>
> - Vous pouvez supprimer des index vectoriels même s'ils contiennent des vecteurs.
> - Tous les vecteurs enregistrés dans l'index sont définitivement supprimés
> - Toutes les métadonnées associées à ces vecteurs sont définitivement perdues
> - L'opération ne peut pas être annulée ou inversée
> - Toute opération en cours sur l'indice échouera immédiatement
> - Les applications interrogeant l'index recevront des erreurs
> - Le nom de l'index devient disponible pour être réutilisé dans le bucket.

En utilisant le AWS CLI

Avant de supprimer un index vectoriel, vérifiez-le. Pour plus d'informations sur la façon de vérifier les détails de l'index, consultez GetIndexle manuel Amazon S3 API Reference. Pour plus d'informations sur la façon de répertorier les vecteurs dans l'index afin de voir ce qui sera supprimé, consultezRépertorier les index vectoriels.

Pour supprimer un index vectoriel, utilisez les exemples de commandes suivants. Remplacez *`user input placeholders`* par vos propres informations.

```
aws s3vectors delete-index --vector-bucket-name "amzn-s3-demo-vector-bucket" \
          --index-name "idx2"
```

Pour plus d'informations sur la façon de vérifier si l'index est supprimé, consultezRépertorier les index vectoriels.

Vecteurs

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Chaque vecteur est constitué d'une clé qui identifie de manière unique chaque vecteur dans un index vectoriel. En outre, vous pouvez associer des métadonnées (par exemple, année, auteur, genre, lieu) sous forme de paires clé-valeur à chaque vecteur.

Les opérations relatives aux données vectorielles incluent l'insertion, le listage, l'interrogation et la suppression de vecteurs. Pour générer de nouvelles intégrations vectorielles de vos données non structurées, vous pouvez utiliser l'InvokeModelopération API d'Amazon Bedrock pour spécifier l'ID du modèle d'intégration que vous souhaitez utiliser. En outre, l'outil open source Amazon S3 Vectors Embed CLI fournit un moyen simplifié de générer des intégrations et d'effectuer des recherches sémantiques à partir de la ligne de commande. Pour plus d'informations sur cet outil open source qui automatise à la fois la génération d'intégrations vectorielles avec les modèles Amazon Bedrock Foundation et les opérations de recherche sémantique dans vos index vectoriels S3, consultez. Création d'intégrations vectorielles et réalisation de recherches sémantiques avec `s3vectors-embed-cli`

Concepts vectoriels

Clés vectorielles : chaque vecteur est identifié par une clé vectorielle unique dans l'index. Les clés vectorielles peuvent comporter jusqu'à 1 024 caractères et doivent être uniques dans l'index vectoriel. Les touches distinguent les majuscules et minuscules et peuvent contenir n'importe quel caractère UTF-8.

Dimension du vecteur : une dimension est le nombre de valeurs d'un vecteur. Les grandes dimensions nécessitent plus d'espace de rangement. Tous les vecteurs d'un index doivent avoir le

même nombre de dimensions, qui est spécifié lors de la création de l'index. Une dimension doit être un entier compris entre 1 et 4096.

Métadonnées : vous pouvez associer des métadonnées aux vecteurs sous forme de paires clé-valeur pour fournir un contexte supplémentaire et activer le filtrage lors des requêtes. Les métadonnées incluent des clés de métadonnées filtrables et non filtrables. Les métadonnées filtrables sont utilisées pour le filtrage des requêtes. Les clés de métadonnées non filtrables sont spécifiées lors de la création d'un index vectoriel et fournissent un contexte supplémentaire mais ne peuvent pas être utilisées pour le filtrage. Les métadonnées prennent en charge les types chaîne, numérique et booléen. Pour plus d'informations sur les métadonnées filtrables et non filtrables, consultez. Filtrage des métadonnées Pour plus d'informations sur les limites de métadonnées, y compris les limites de taille par vecteur et le nombre maximal de clés de métadonnées par vecteur, voir Limitations et restrictions.

Rubriques

- Insertion de vecteurs dans un index vectoriel
- Vecteurs de listes
- Vecteurs d'interrogation
- Supprimer des vecteurs d'un index vectoriel
- Filtrage des métadonnées

Insertion de vecteurs dans un index vectoriel

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez ajouter des vecteurs à un index vectoriel à l'aide de l'opération PutVectorsAPI. Chaque vecteur est constitué d'une clé qui identifie de manière unique chaque vecteur dans un index vectoriel. Si vous insérez un vecteur avec une clé qui existe déjà dans l'index, il remplacera complètement le vecteur existant, ce qui rend le vecteur précédent impossible à rechercher. Pour optimiser le débit d'écriture, il est recommandé d'insérer des vecteurs par lots volumineux, jusqu'à la taille de lot maximale pour. `PutVectors` Pour plus d'informations sur la taille de lot maximale pour`PutVectors`, qui est la limite de vecteurs par appel d'`PutVectors`API, consultezLimites et

restrictions. En outre, vous pouvez joindre des métadonnées (par exemple, année, auteur, genre, lieu) sous forme de paires clé-valeur à chaque vecteur. Par défaut, toutes les clés de métadonnées associées aux vecteurs sont filtrables et peuvent être utilisées comme filtres dans une requête de similarité. Seules les clés de métadonnées spécifiées comme non filtrables lors de la création de l'index vectoriel sont exclues du filtrage. Les index vectoriels S3 prennent en charge les types de métadonnées de type chaîne, numérique, booléen et liste. Pour plus d'informations sur la limite de taille totale des métadonnées par vecteur et la limite de taille des métadonnées filtrables par vecteur, consultezLimites et restrictions. Si la taille des métadonnées dépasse ces limites, l'opération d'`PutVectors`API renvoie une `400 Bad Request` erreur.

Avant d'ajouter des données vectorielles à votre index vectoriel à l'aide de l'opération `PutVectors` API, vous devez convertir vos données brutes en intégrations vectorielles, qui sont des représentations numériques de votre contenu sous forme de tableaux de nombres à virgule flottante. Les intégrations vectorielles capturent la signification sémantique de votre contenu, permettant ainsi des recherches de similarité une fois qu'elles sont stockées dans votre index vectoriel pendant l'opération. `PutVectors` Vous pouvez générer des intégrations vectorielles à l'aide de différentes méthodes en fonction de votre type de données et de votre cas d'utilisation. Ces méthodes incluent l'utilisation de frameworks d'apprentissage automatique, de bibliothèques d'intégration spécialisées ou de AWS services tels qu'Amazon Bedrock. Par exemple, si vous utilisez Amazon Bedrock, vous pouvez générer des intégrations à l'aide de l'opération InvokeModelAPI et de votre modèle d'intégration préféré.

En outre, les bases de connaissances Amazon Bedrock fournissent un flux de travail end-to-end RAG entièrement géré dans lequel Amazon Bedrock récupère automatiquement les données de votre source de données S3, convertit le contenu en blocs de texte, génère des intégrations et les stocke dans votre index vectoriel. Vous pouvez ensuite interroger la base de connaissances et générer des réponses basées sur des fragments extraits de vos données sources.

En outre, l'outil open source Amazon S3 Vectors Embed CLI fournit un moyen simplifié de générer des intégrations et d'effectuer des recherches sémantiques à partir de la ligne de commande. Pour plus d'informations sur cet outil open source qui automatise à la fois la génération d'intégrations vectorielles avec les modèles Amazon Bedrock Foundation et les opérations de recherche sémantique dans vos index vectoriels S3, consultez. Création d'intégrations vectorielles et réalisation de recherches sémantiques avec `s3vectors-embed-cli`

> **Note**
>
> Lorsque vous insérez des données vectorielles dans votre index vectoriel, vous devez fournir les données vectorielles sous forme de valeurs `float32` (virgule flottante 32 bits). Si vous transmettez des valeurs plus précises à un AWS SDK, S3 Vectors les convertit en virgule flottante 32 bits avant de les stocker GetVectorsListVectors, et les QueryVectorsopérations renvoient les valeurs. `float32` Différents AWS SDKs peuvent avoir des types numériques par défaut différents. Assurez-vous donc que vos vecteurs sont correctement formatés en tant que `float32` valeurs, quel que soit le SDK que vous utilisez. Par exemple, en Python, utilisez `numpy.float32` ou convertissez explicitement vos valeurs.

À l'aide du AWS SDKs

SDK for Python

```
# Populate a vector index with embeddings from Amazon Titan Text Embeddings V2.
import boto3
import json

# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Texts to convert to embeddings.
texts = [
    "Star Wars: A farm boy joins rebels to fight an evil empire in space",
    "Jurassic Park: Scientists create dinosaurs in a theme park that goes wrong",
    "Finding Nemo: A father fish searches the ocean to find his lost son"
]

# Generate vector embeddings.
embeddings = []
for text in texts:
    response = bedrock.invoke_model(
        modelId="amazon.titan-embed-text-v2:0",
        body=json.dumps({"inputText": text})
    )

    # Extract embedding from response.
    response_body = json.loads(response["body"].read())
```

```
    embeddings.append(response_body["embedding"])

# Write embeddings into vector index with metadata.
s3vectors.put_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    vectors=[
        {
            "key": "Star Wars",
            "data": {"float32": embeddings[0]},
            "metadata": {"source_text": texts[0], "genre":"scifi"}
        },
        {
            "key": "Jurassic Park",
            "data": {"float32": embeddings[1]},
            "metadata": {"source_text": texts[1], "genre":"scifi"}
        },
        {
            "key": "Finding Nemo",
            "data": {"float32": embeddings[2]},
            "metadata": {"source_text": texts[2], "genre":"family"}
        }
    ]
)
```

Vecteurs de listes

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez répertorier les vecteurs dans un index vectoriel à l'aide de l'opération ListVectorsAPI. Pour plus d'informations sur le nombre maximal de vecteurs pouvant être renvoyés par page, consultezLimites et restrictions. La réponse inclut un jeton de pagination lorsque les résultats sont tronqués. Pour plus d'informations sur les éléments de réponse de`ListVectors`, consultez ListVectorsle manuel Amazon S3 API Reference. Vous pouvez également l'utiliser `ListVectors` pour exporter des données vectorielles à partir d'un index vectoriel spécifié. `ListVectors`est très

cohérent. Après une opération WRITE, vous pouvez immédiatement répertorier les vecteurs avec toutes les modifications reflétées.

À l'aide du AWS CLI

Pour répertorier les vecteurs, utilisez les exemples de commandes suivants. Remplacez *`user input placeholders`* par vos propres informations.

Les `segment-index` paramètres `segment-count` et vous permettent de partitionner vos opérations de référencement sur plusieurs requêtes parallèles. Lorsque vous spécifiez une `segment-count` valeur (telle que2), vous divisez l'index en autant de segments. Le `segment-index` paramètre (à partir de 0) détermine le segment à répertorier. Cette approche permet d'améliorer les performances lors de la liste de grands index vectoriels en activant le traitement parallèle. Pour plus d'informations sur `segment-count` et`segment-index`, consultez ListVectorsle manuel de référence des API Amazon S3.

Pour répertorier tous les vecteurs dans un index

Exemple de demande :

```
aws s3vectors list-vectors \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --index-name "idx" \
  --segment-count 2 \
  --segment-index 0 \
  --return-data \
  --return-metadata
```

Exemple de réponse :

```
{
    "vectors": [
        {
            "key": "vec3",
            "data": {
                "float32": [0.4000000059604645]
            },
            "metadata": {
                "nonFilterableKey": "val4",
                "filterableKey": "val2"
            }
        }
```

```
    ]
}
```

Pour répertorier les vecteurs avec pagination

Exemple de demande :

```
aws s3vectors list-vectors \
  --vector-bucket-name "amzn-s3-demo-vector-bucket" \
  --index-name "idx" \
  --segment-count 2 \
  --segment-index 0 \
  --return-data \
  --return-metadata \
  --next-token
 "zWfh7e57H2jBfBtRRmC7OfMwl209G9dg3j2qM6kM4t0rps6ClYzJykgMOil9eGqU5nhf_gTq53IfoUdTnsg"
```

Exemple de réponse :

```
{
    "vectors": [
        {
            "key": "vec1",
            "data": {
                "float32": [0.5]
            },
            "metadata": {
                "nonFilterableKey": "val2",
                "filterableKey": "val1"
            }
        }
    ]
}
```

Vecteurs d'interrogation

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez exécuter une requête de similarité à l'aide de l'opération QueryVectorsAPI, dans laquelle vous spécifiez le vecteur de requête, le nombre de résultats pertinents à renvoyer (les K voisins les plus proches) et l'ARN de l'index. En outre, vous pouvez utiliser des filtres de métadonnées dans une requête pour rechercher uniquement les vecteurs correspondant au filtre. Si vous faites une demande de filtrage sur un champ de métadonnées non filtrable, la demande renverra une `400 Bad Request` erreur. Pour plus d'informations sur le filtrage des métadonnées, consultezFiltrage des métadonnées.

Dans la réponse, les clés vectorielles sont renvoyées par défaut. Vous pouvez éventuellement inclure la distance et les métadonnées dans la réponse.

Lorsque vous générez le vecteur de requête, vous devez utiliser le même modèle d'intégration de vecteurs que celui utilisé pour générer les vecteurs initiaux stockés dans l'index vectoriel. Par exemple, si vous utilisez le modèle Amazon Titan Text Embeddings V2 dans Amazon Bedrock pour générer des intégrations vectorielles de vos documents, utilisez le même modèle d'intégration pour convertir une question en vecteur de requête. En outre, les bases de connaissances Amazon Bedrock fournissent un flux de travail end-to-end RAG entièrement géré dans lequel Amazon Bedrock récupère automatiquement les données de votre source de données S3, convertit le contenu en blocs de texte, génère des intégrations et les stocke dans votre index vectoriel. Vous pouvez ensuite interroger la base de connaissances et générer des réponses basées sur des fragments extraits de vos données sources. Pour plus d'informations sur la façon d'interroger des vecteurs à partir d'une base de connaissances Amazon Bedrock dans la console, consultez(Facultatif) Intégrez les vecteurs S3 aux bases de connaissances Amazon Bedrock.

En outre, l'outil open source Amazon S3 Vectors Embed CLI fournit un moyen simplifié d'effectuer des recherches sémantiques à partir de la ligne de commande. Cet outil open source rationalise le processus de requête en gérant à la fois la génération d'intégration vectorielle avec les modèles Amazon Bedrock Foundation et en exécutant des opérations de recherche sémantique sur vos index vectoriels S3. Pour plus d'informations sur l'utilisation de cet outil pour interroger vos données vectorielles, consultezCréation d'intégrations vectorielles et réalisation de recherches sémantiques avec `s3vectors-embed-cli`.

S3 Vectors fournit des temps de latence de requête inférieurs à une seconde. S3 Vectors utilise le débit élastique d'Amazon S3 pour gérer les recherches sur des millions de vecteurs et est idéal pour les charges de travail où les requêtes sont moins fréquentes. Lorsque vous effectuez des requêtes de similarité pour vos intégrations vectorielles, plusieurs facteurs peuvent affecter les performances de rappel moyennes, notamment le modèle d'intégration vectorielle, la taille du jeu de données vectorielles (le nombre de vecteurs et de dimensions) et la distribution des requêtes. S3 Vectors

fournit un taux de rappel moyen supérieur à 90 % pour la plupart des ensembles de données. Le rappel moyen mesure la qualité des résultats des requêtes. Un rappel moyen de 90 % signifie que la réponse contient 90 % des vecteurs les plus proches réels (vérité fondamentale) qui sont stockés dans l'index vectoriel relatif au vecteur de requête. Cependant, étant donné que les performances réelles peuvent varier en fonction de vos cas d'utilisation spécifiques, nous vous recommandons d'effectuer vos propres tests avec des données et des requêtes représentatives afin de valider que les vecteurs S3 répondent à vos exigences de rappel.

À l'aide du AWS SDKs

SDK for Python

```
# Query a vector index with an embedding from Amazon Titan Text Embeddings V2.
import boto3
import json

# Create Bedrock Runtime and S3 Vectors clients in the AWS Region of your choice.
bedrock = boto3.client("bedrock-runtime", region_name="us-west-2")
s3vectors = boto3.client("s3vectors", region_name="us-west-2")

# Query text to convert to an embedding.
input_text = "adventures in space"

# Generate the vector embedding.
response = bedrock.invoke_model(
    modelId="amazon.titan-embed-text-v2:0",
    body=json.dumps({"inputText": input_text})
)

# Extract embedding from response.
model_response = json.loads(response["body"].read())
embedding = model_response["embedding"]

# Query vector index.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    returnDistance=True,
    returnMetadata=True
)
print(json.dumps(response["vectors"], indent=2))
```

```
# Query vector index with a metadata filter.
response = s3vectors.query_vectors(
    vectorBucketName="media-embeddings",
    indexName="movies",
    queryVector={"float32": embedding},
    topK=3,
    filter={"genre": "scifi"},
    returnDistance=True,
    returnMetadata=True
)
print(json.dumps(response["vectors"], indent=2))
```

Supprimer des vecteurs d'un index vectoriel

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Vous pouvez supprimer des vecteurs spécifiques d'un index vectoriel en spécifiant leurs clés vectorielles. Cette opération est utile pour supprimer les données périmées ou incorrectes tout en préservant le reste de vos données vectorielles.

À l'aide du AWS CLI

Pour supprimer des vecteurs, utilisez les exemples de commandes suivants. Remplacez *`user input placeholders`* par vos propres informations.

```
aws s3vectors delete-vectors \
 --vector-bucket-name "amzn-s3-demo-vector-bucket" \
 --index-name "idx" \
 --keys '["vec2","vec3"]'
```

Filtrage des métadonnées

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Le filtrage des métadonnées vous permet de filtrer les résultats des requêtes en fonction d'attributs spécifiques attachés à vos vecteurs. Vous pouvez utiliser des filtres de métadonnées avec des opérations de requête pour trouver des vecteurs répondant à la fois à des critères de similarité et à des conditions de métadonnées spécifiques.

S3 Vectors prend en charge deux types de métadonnées : les métadonnées filtrables et les métadonnées non filtrables. La principale différence réside dans le fait que les métadonnées filtrables peuvent être utilisées dans les filtres de requêtes, mais qu'elles sont soumises à des limites de taille plus strictes, tandis que les métadonnées non filtrables ne peuvent pas être utilisées dans les filtres mais peuvent stocker de plus grandes quantités de données dans les limites de taille fixées. Pour plus d'informations sur les limites de métadonnées, notamment les limites de taille par vecteur et le nombre maximal de clés de métadonnées par vecteur, consultezLimites et restrictions.

Rubriques

- Métadonnées filtrables
- Exemples de métadonnées filtrables valides
- Métadonnées non filtrables

Métadonnées filtrables

Les métadonnées filtrables vous permettent de filtrer les résultats des requêtes en fonction de valeurs de métadonnées spécifiques. Par défaut, tous les champs de métadonnées sont filtrables dans une requête de similarité, sauf s'ils sont explicitement spécifiés comme non filtrables lors de la création de l'index vectoriel. S3 Vectors prend en charge les types de métadonnées de type chaîne, numérique, booléen et liste avec une limite de taille par vecteur. Le type de métadonnées est idéal pour les attributs que vous souhaitez filtrer, tels que les catégories, les horodatages ou les valeurs de statut.

Si la taille des métadonnées dépasse les limites prises en charge, l'opération d'PutVectorsAPI renvoie une `400 Bad Request` erreur. Pour plus d'informations sur la limite de taille des métadonnées filtrables par vecteur, consultezLimites et restrictions.

Les opérations suivantes peuvent être utilisées avec des métadonnées filtrables.

Opérateur	Types d'entrée valides	Description
`$eq`	Chaîne, nombre, booléen	Comparaison des correspondances exactes pour des valeurs uniques. Lors de la comparaison avec une valeur de métadonnées de tableau, renvoie `true` si la valeur d'entrée correspond à un élément du tableau. Par exemple, `{"category": {"$eq": "documentary"}}` ferait correspondre un vecteur à des métadonnées`"category": ["documentary", "romance"]` .
`$ne`	Chaîne, nombre, booléen	Comparaison inégale
`$gt`	Nombre	Plus que la comparaison
`$gte`	Nombre	Comparaison supérieure ou égale
`$lt`	Nombre	Moins qu'une comparaison
`$lte`	Nombre	Comparaison inférieure ou égale
`$in`	Tableau de primitives non vide	Correspond à n'importe quelle valeur du tableau

Opérateur	Types d'entrée valides	Description
`$nin`	Tableau de primitives non vide	Ne correspond à aucune des valeurs du tableau
`$exists`	Booléen	Vérifiez si le champ existe
`$and`	Tableau de filtres non vide	ET logique de plusieurs conditions
`$or`	Tableau de filtres non vide	OR logique de plusieurs conditions

Exemples de métadonnées filtrables valides

Égalité simple

```
{"genre": "documentary"}
```

Ce filtre correspond aux vecteurs dont la clé de métadonnées du genre est égale à « documentaire ». Lorsque vous ne spécifiez aucun opérateur, S3 Vectors utilise automatiquement l'opérateur $eq.

Égalité explicite

```
// Example: Exact match
{"genre": {"$eq": "documentary"}}
```

```
// Example: Not equal to
{"genre": {"$ne": "drama"}}
```

Comparaison numérique

```
{"year": {"$gt": 2019}}
```

```
{"year": {"$gte": 2020}}
```

```
{"year": {"$lt": 2020}}
```

```
{"year": {"$lte": 2020}}
```

Opérations sur les réseaux

```
{"genre": {"$in": ["comedy", "documentary"]}}
```

```
{"genre": {"$nin": ["comedy", "documentary"]}}
```

Contrôle d'existence

```
{"genre": {"$exists": true}}
```

Le `$exists` filtre fait correspondre les vecteurs dotés d'une clé de métadonnées « genre », quelle que soit la valeur stockée pour cette clé de métadonnées.

Opérations logiques

```
{"$and": [{"genre": {"$eq": "drama"}}, {"year": {"$gte": 2020}}]}
```

```
{"$or": [{"genre": {"$eq": "drama"}}, {"year": {"$gte": 2020}}]}
```

Fourchette de prix (plusieurs conditions sur le même champ)

```
{"price": {"$gte": 10, "$lte": 50}}
```

Pour plus d'informations sur la manière d'interroger des vecteurs à l'aide du filtrage des métadonnées, consultezFiltrage des métadonnées.

Métadonnées non filtrables

Les métadonnées non filtrables ne peuvent pas être utilisées dans les filtres de requête, mais elles peuvent stocker de plus grandes quantités de données contextuelles que les métadonnées filtrables. Il est idéal pour stocker de gros morceaux de texte, des descriptions détaillées ou d'autres informations contextuelles qui n'ont pas besoin d'être consultables mais qui peuvent être renvoyées avec les résultats de la requête. Par exemple, vous pouvez stocker le texte complet du document, les descriptions d'images ou les spécifications détaillées des produits sous forme de métadonnées non filtrables.

Les clés de métadonnées non filtrables doivent être configurées de manière explicite lors de la création de l'index vectoriel. Une fois qu'une clé de métadonnées est désignée comme non filtrable lors de la création de l'index, elle ne peut pas être modifiée pour être filtrée ultérieurement. Vous pouvez configurer plusieurs clés de métadonnées comme non filtrables par index vectoriel, chaque nom de clé de métadonnées étant limité à 63 caractères. Pour plus d'informations sur le nombre maximal de clés de métadonnées non filtrables autorisées par index vectoriel, consultez. Limites et restrictions

Bien que vous ne puissiez pas filtrer les métadonnées non filtrables, vous pouvez les récupérer avec les résultats des requêtes à l'aide du `return-metadata` paramètre. Vous pouvez utiliser des métadonnées non filtrables pour certains cas d'utilisation, comme suit.

- Utilisez-le pour fournir un contexte à votre application sans analyser des sources de données distinctes.
- Stockez des blocs de texte plus volumineux qui dépasseraient les limites de taille des métadonnées filtrables.
- Incluez-le dans les exportations vectorielles à l'aide de l'opération ListVectorsAPI.

Pour plus d'informations sur la configuration de métadonnées non filtrables, consultez. Création d'un index vectoriel dans un compartiment vectoriel

Limites et restrictions

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Amazon S3 Vectors comporte certaines limites et restrictions dont vous devez tenir compte lors de la planification de vos applications de stockage et de recherche de vecteurs.

- Compartiments vectoriels par AWS région dans un compte : 10 000
- Index vectoriels par compartiment vectoriel : 10 000
- Vecteurs par indice vectoriel : jusqu'à 50 millions
- Valeur de dimension par vecteur : 1 à 4 096

- Total des métadonnées par vecteur : jusqu'à 40 Ko (filtrable et non filtrable)
- Nombre total de clés de métadonnées par vecteur : jusqu'à 10
- Métadonnées filtrables par vecteur : jusqu'à 2 Ko
- Clés de métadonnées non filtrables par index vectoriel : jusqu'à 10
- Demandes d'écriture par seconde et par index vectoriel : jusqu'à 5
- Taille de la charge utile de la demande : jusqu'à 20 MiB
- Vecteurs par appel d'PutVectorsAPI : jusqu'à 500
- Vecteurs par appel d'DeleteVectorsAPI : jusqu'à 500
- Vecteurs par appel d'GetVectorsAPI : jusqu'à 100
- Top K des résultats par QueryVectorsdemande : jusqu'à 30
- Vecteurs listés par page dans une ListVectorsréponse : jusqu'à 1 000
- Buckets vectoriels listés par page dans une ListVectorBucketsréponse : jusqu'à 500.
- Index vectoriels listés par page dans une ListIndexesréponse : jusqu'à 500.
- Nombre de segments pour le listing parallèle : jusqu'à 16

Si vous avez besoin de limites plus élevées, contactez l'équipe chargée de votre AWS compte.

Meilleures pratiques en matière de vecteurs S3

Amazon S3 Vectors fournit un stockage vectoriel spécialement conçu et optimisé en termes de coûts, destiné aux applications basées sur l'IA et à la recherche sémantique de votre contenu stocké dans Amazon S3. Conçu pour fournir une élasticité et une durabilité de niveau S3 pour le stockage d'ensembles de données vectorielles avec des performances de requête inférieures à la seconde, S3 Vectors est idéal pour les applications qui doivent créer et développer des index vectoriels. Avec S3 Vectors, vous pouvez utiliser un ensemble dédié d'opérations d'API pour stocker, accéder et exécuter des requêtes de similarité sur des données vectorielles sans fournir d'infrastructure. Pour de plus amples informations, veuillez consulter Utilisation de vecteurs S3 et de buckets vectoriels.

Pour tirer le meilleur parti des vecteurs S3, nous vous recommandons de suivre les meilleures pratiques suivantes.

Insertion et suppression de vecteurs

Votre application peut atteindre au moins cinq DeleteVectorsrequêtes par seconde PutVectorset par index vectoriel. Si vous dépassez le taux de demandes, il est possible que vous receviez un `429 TooManyRequestsException` message d'erreur. Pour optimiser le débit des demandes et optimiser la vitesse et l'efficacité, nous vous recommandons d'insérer et de supprimer des vecteurs par lots importants, jusqu'à un maximum de 500 vecteurs par demande d'API. Pour de plus amples informations, veuillez consulter Indices vectoriels.

Accès et interrogation de vecteurs dans un index vectoriel S3

Votre application peut traiter des centaines de QueryVectorsListVectorsrequêtes par seconde par index vectoriel S3. GetVectors Si vous dépassez le taux de demandes, il est possible que vous receviez un `429 TooManyRequestsException` message d'erreur. Nous vous recommandons d'utiliser un mécanisme de nouvelle tentative et de configurer votre application pour qu'elle envoie moins de demandes.

Mise à l'échelle des index vectoriels

Pour améliorer les performances des requêtes par index vectoriel, pensez à configurer votre application pour diviser les vecteurs sur plusieurs index vectoriels lorsque cela est possible. Par exemple, si vous avez des charges de travail multi-locataires et que votre application interroge chaque locataire indépendamment, envisagez de stocker les vecteurs de chaque locataire dans un index vectoriel distinct. Pour de plus amples informations, veuillez consulter Indices vectoriels.

Implémentation de la mutualisation avec des index vectoriels distincts

Vous pouvez obtenir la mutualisation en organisant vos données vectorielles à l'aide d'un index vectoriel unique pour chaque locataire. Vous pouvez utiliser les politiques IAM et de bucket pour restreindre l'accès de chaque locataire uniquement à son index vectoriel désigné. Cette approche permet de préserver l'isolation des données et de simplifier la gestion en éliminant la nécessité de créer des compartiments distincts pour chaque locataire. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès dans S3 Vectors.

Configuration de champs de métadonnées non filtrables pour les index vectoriels

Lorsque vous créez un index vectoriel, configurez les champs de métadonnées qui ne nécessitent pas de filtrage en tant que clés de métadonnées non filtrables. Par exemple, stockez des fragments de texte pour les intégrations vectorielles sous forme de champs de métadonnées non filtrables lorsque vous en avez besoin uniquement à titre de référence. Pour de plus amples informations, veuillez consulter Métadonnées non filtrables.

Création d'intégrations vectorielles et réalisation de recherches sémantiques avec **`s3vectors-embed-cli`**

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Amazon S3 Vectors fournit un outil open source autonome appelé Amazon S3 Vectors Embed CLI `s3vectors-embed-cli` () qui simplifie l'utilisation des données vectorielles en combinant la génération d'intégration avec les opérations vectorielles dans des commandes uniques. Cet outil CLI vous permet de démarrer rapidement avec les vecteurs S3 en automatisant la génération d'intégrations vectorielles avec les modèles de base Amazon Bedrock et les opérations de recherche sémantique dans vos index vectoriels.

La CLI S3 Vectors Embed fournit deux commandes principales pour intégrer les modèles d'intégration Amazon Bedrock aux opérations S3 Vectors :

- `s3vectors-embed put`: générez et insérez des intégrations vectorielles dans un index vectoriel. Plus précisément, convertissez le texte et les images en intégrations vectorielles via les modèles Amazon Bedrock et stockez-les automatiquement dans votre index vectoriel.
- `s3vectors-embed query`: générez des intégrations vectorielles à partir de votre requête via les modèles Amazon Bedrock et des vecteurs de requête dans votre index vectoriel.

La CLI Amazon S3 Vectors Embed est disponible dans le GitHub référentiel Amazon Web Services - Labs. Pour obtenir des instructions d'installation détaillées, des paramètres de commande, des exemples et des meilleures pratiques, consultez le GitHub référentiel Amazon S3 Vectors Embed CLI.

Pour les opérations d'API S3 Vectors de niveau inférieur qui offrent davantage de contrôle et de personnalisation, consultez Amazon S3 Vectors dans le manuel Amazon Simple Storage Service API Reference.

Utilisation de vecteurs S3 avec d'autres AWS services

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

S3 Vectors s'intègre à d'autres AWS services pour améliorer vos capacités de traitement vectoriel et fournir des solutions complètes pour les charges de travail liées à l'IA et à l'apprentissage automatique. Ces intégrations vous permettent de tirer parti du stockage rentable des vecteurs S3 ainsi que des fonctionnalités spécialisées d'autres AWS services.

Intégrations disponibles

S3 Vectors fournit des intégrations natives avec les AWS services suivants :

- Amazon OpenSearch Service- Vous pouvez exporter un instantané d'un index vectoriel vers Amazon OpenSearch Service pour les recherches vectorielles à haut taux de requêtes par seconde (QPS) et à faible latence. Amazon OpenSearch Service Ajoute également Amazon S3 Vectors en tant que nouveau moteur économique pour les clients qui souhaitent optimiser les coûts tout en continuant à utiliser les opérations d' Amazon OpenSearch Service API pour des

fonctionnalités de recherche avancées, notamment la recherche hybride, les agrégations, le filtrage avancé, la recherche à facettes, etc.

- Amazon Bedrock Bases de connaissances - Utilisez les vecteurs S3 comme magasin de vecteurs pour les applications RAG (Retrieval Augmented Generation), réduisant ainsi les coûts de stockage tout en préservant les performances des requêtes pour les opérations de base de connaissances. Vous pouvez accéder à cette intégration via la console Amazon Bedrock ou Amazon SageMaker AI Unified Studio.

Avantages de l'intégration

Ces intégrations présentent plusieurs avantages essentiels :

- Optimisation des coûts : stockez de grands ensembles de données vectorielles de manière rentable dans S3 Vectors tout en utilisant des services spécialisés pour des charges de travail spécifiques, comme Amazon OpenSearch pour les fonctionnalités de recherche avancées.
- Flexibilité des performances : choisissez l'intégration adaptée à vos exigences en matière de performances : vecteurs S3 pour le stockage à faible débit et les requêtes sporadiques, et autres services pour les opérations à haut débit et à faible latence.
- Intégration du flux de travail : intégrez facilement les opérations vectorielles dans les pipelines existants AWS basés sur l'IA et le ML.
- Gestion simplifiée : réduisez la complexité opérationnelle en utilisant des intégrations gérées plutôt que de créer des solutions personnalisées.

Rubriques

- Utilisation de vecteurs S3 avec OpenSearch Service
- Utilisation de vecteurs S3 avec les bases de connaissances Amazon Bedrock

Utilisation de vecteurs S3 avec OpenSearch Service

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Amazon S3 Vectors s'intègre OpenSearch pour fournir des fonctionnalités de stockage et de recherche vectorielles flexibles. Cette intégration vous permet d'optimiser les coûts en stockant les vecteurs dans S3 Vectors tout en tirant parti des fonctionnalités de recherche avancées de OpenSearch.

Il existe deux intégrations entre S3 Vectors et OpenSearch. La première consiste à exporter des données vectorielles de S3 Vectors vers OpenSearch Serverless pour des capacités de recherche performantes. L'autre utilise S3 Vectors comme moteur de stockage rentable tout OpenSearch en conservant l'accès aux OpenSearch fonctionnalités.

Exporter vers OpenSearch Serverless

Vous pouvez exporter des index vectoriels de S3 Vectors vers des collections OpenSearch sans serveur pour des opérations de recherche hautes performances, des recherches hybrides, des agrégations, un filtrage avancé et une recherche à facettes. Lorsque vous exportez, les données sont copiées vers OpenSearch Serverless tout en restant dans S3 Vectors, ce qui signifie que vous devrez payer pour les deux services pendant cette période.

Quand utiliser cette intégration

Envisagez d'exporter vers OpenSearch Serverless à partir de S3 Vectors lorsque vous avez besoin des éléments suivants :

- Fonctionnalités de recherche hybrides qui combinent similarité vectorielle et recherche par mots clés.
- Débit de requêtes élevé pour les charges de travail exigeantes.
- Réponses à faible latence pour les applications en temps réel qui nécessitent des temps de réponse en millisecondes.
- Analyses avancées qui incluent les agrégations, la recherche à facettes et le filtrage complexe.

Prérequis

Avant d'utiliser des vecteurs S3 avec OpenSearch, assurez-vous de disposer des éléments suivants :

- Un compartiment vectoriel S3 existant avec des index vectoriels contenant vos données.
- Autorisations IAM appropriées pour les vecteurs et le OpenSearch service S3.
- Compréhension de vos exigences de performance pour choisir la méthode d'intégration appropriée.

Premiers pas

En utilisant le AWS Management Console

Pour exporter des données vectorielles vers OpenSearch

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Vector buckets.
3. Dans la liste des compartiments vectoriels, choisissez le nom du compartiment contenant les données vectorielles que vous souhaitez exporter.
4. Pour les index vectoriels, cliquez sur le bouton radio situé à côté de l'index vectoriel que vous souhaitez exporter.
5. Choisissez Exporter par recherche avancée, puis Exporter vers OpenSearch.

⚠ Important

- Point-in-time export : L'export capture les données jusqu'au lancement de l'export. Si vous mettez à jour vos données vectorielles pendant l'ingestion OpenSearch, toutes les mises à jour ne seront pas reflétées dans OpenSearch.
- Opération unique : il s'agit d'une exportation unique qui ne restera pas synchronisée avec vos données S3 Vectors. Vous devez réexporter manuellement pour enregistrer les modifications ultérieures.

Ensuite, pour configurer et gérer l'intégration des vecteurs S3 à Amazon OpenSearch Service, vous travaillerez principalement via la OpenSearch console.

Pour afficher les exportations vers OpenSearch

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Vector buckets.
3. Dans la liste des compartiments vectoriels, choisissez le nom du compartiment contenant les données vectorielles que vous souhaitez exporter.

4. Pour les index vectoriels, choisissez Exporter la recherche avancée, puis Afficher les exportations vers OpenSearch.

Ensuite, vous verrez les exportations vers OpenSearch via la OpenSearch console.

Pour plus d'informations sur la création et la gestion de collections OpenSearch sans serveur, consultez la section Création et gestion de collections Amazon OpenSearch Service Serverless dans le manuel Amazon OpenSearch Service Developer Guide.

OpenSearch avec le moteur S3 Vectors

Vous pouvez utiliser S3 Vectors comme moteur de stockage sous-jacent pour les clusters OpenSearch gérés par Amazon, afin de fournir un stockage vectoriel optimisé en termes de coûts tout en préservant les OpenSearch fonctionnalités.

Quand utiliser cette intégration

Envisagez de l'utiliser OpenSearch avec le moteur S3 Vectors lorsque vous avez besoin des éléments suivants :

- Fonctionnalités de recherche hybrides qui combinent similarité vectorielle et recherche par mots clés.
- Débit de requêtes réduit, ce qui peut entraîner des modèles d'utilisation moins fréquents ou sporadiques.
- Tolérance de latence plus élevée pour les applications qui peuvent accepter des temps de réponse plus longs en échange d'économies de coûts.
- Analyses avancées qui incluent les agrégations, la recherche à facettes et le filtrage complexe.
- OpenSearch Workflows existants que vous souhaitez étendre grâce à un stockage vectoriel rentable.

Prérequis

Avant de l'utiliser OpenSearch avec le moteur S3 Vectors, assurez-vous d'avoir :

- Un domaine OpenSearch géré existant. Pour plus d'informations, consultez la section Création et gestion de domaines Amazon OpenSearch Service dans le manuel Amazon OpenSearch Service Developer Guide.

- Compréhension de vos exigences de performance pour choisir la méthode d'intégration appropriée.

Démarrage

Pour l'utiliser OpenSearch avec le moteur S3 Vectors, configurez votre moteur sur `S3_Vectors` lors de la création de l'index dans OpenSearch. Pour plus d'informations sur le modèle que vous utilisez lors de la création d'un index dans OpenSearch Service, notamment sur l'endroit où spécifier le type de moteur, consultez la section Méthodes et moteurs. Pour plus d'informations sur l'intégration entre le moteur de vecteurs S3 OpenSearch et le moteur de vecteurs S3, consultez la section Fonctionnalités de recherche avancées avec un moteur de vecteurs S3 dans le manuel Amazon OpenSearch Service Developer Guide.

Utilisation de vecteurs S3 avec les bases de connaissances Amazon Bedrock

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

S3 Vectors s'intègre aux bases de connaissances Amazon Bedrock et à Amazon SageMaker AI Unified Studio afin de simplifier et de réduire le coût du stockage vectoriel pour les applications de génération augmentée (RAG) par récupération.

Pour plus d'informations sur les commandes CLI de haut niveau qui intègrent les modèles d'intégration Amazon Bedrock aux opérations S3 Vectors, consultez.

Rubriques

- Présentation de l'intégration
- Quand utiliser cette intégration
- Modèles d'intégration pris en charge
- Conditions préalables et autorisations
- Création d'une base de connaissances avec des vecteurs S3
- Gestion et consultation de votre base de connaissances

- Limites

Présentation de l'intégration

Lorsque vous créez une base de connaissances dans Amazon Bedrock, vous pouvez sélectionner S3 Vectors comme magasin de vecteurs. Cette intégration fournit les éléments suivants :

- Économies de coûts pour les applications RAG utilisant de grands ensembles de données vectorielles.
- Intégration parfaite avec le flux de travail RAG entièrement géré d'Amazon Bedrock.
- Gestion automatique des vecteurs gérée par le service Amazon Bedrock.
- Latence de requête inférieure à une seconde pour les opérations de récupération de la base de connaissances.

Les bases de connaissances Amazon Bedrock fournissent un flux de travail end-to-end RAG entièrement géré. Lorsque vous créez une base de connaissances avec S3 Vectors, Amazon Bedrock extrait automatiquement les données de votre source de données S3, convertit le contenu en blocs de texte, génère des intégrations et les stocke dans votre index vectoriel. Vous pouvez ensuite interroger la base de connaissances et générer des réponses basées sur des fragments extraits de vos données sources.

Quand utiliser cette intégration

Envisagez d'utiliser des vecteurs S3 avec les bases de connaissances Amazon Bedrock lorsque vous avez besoin des éléments suivants :

- Stockage vectoriel rentable pour les grands ensembles de données où le temps de latence des requêtes inférieur à une seconde répond aux exigences de votre application.
- Récupération de documents basée sur du texte et des images pour des cas d'utilisation tels que la recherche dans les manuels, les politiques et le contenu visuel.
- Applications RAG qui privilégient l'optimisation des coûts de stockage par rapport aux réponses à très faible latence.
- Gestion des opérations vectorielles sans avoir à apprendre directement les opérations de l'API S3 Vectors. Vous pouvez continuer à utiliser les interfaces Amazon Bedrock que vous connaissez déjà.
- Stockage vectoriel à long terme associé à la durabilité et à l'évolutivité d'Amazon S3

Cette intégration est idéale pour les entreprises qui créent des applications RAG qui ont besoin de rechercher et d'extraire des informations à partir de contenus écrits et d'images, pour lesquelles les avantages économiques des vecteurs S3 correspondent à des exigences de performances de requête acceptables.

Modèles d'intégration pris en charge

L'intégration de S3 Vectors aux bases de connaissances Amazon Bedrock prend en charge les modèles d'intégration suivants :

- amazon. titan-embed-text-v2:0 - Pour les intégrations basées sur du texte
- amazon. titan-embed-image-v1 - Pour les intégrations d'images et multimodales
- cohérer. embed-english-v3 - Pour les intégrations de texte multilingues et spécialisées

Conditions préalables et autorisations

Avant de créer une base de connaissances avec S3 Vectors, assurez-vous de disposer des éléments suivants :

- Autorisations IAM appropriées pour les services S3 Vectors et Amazon Bedrock. Pour plus d'informations sur les autorisations IAM pour les vecteurs S3, consultezthe section called "Gestion des identités et des accès dans S3 Vectors". Pour plus d'informations sur les autorisations IAM associées à votre rôle de service Amazon Bedrock Knowledge Bases afin d'accéder aux vecteurs S3, consultez la section Autorisations d'accès à votre boutique vectorielle dans Amazon S3 Vectors dans le guide de l'utilisateur d'Amazon Bedrock.
- Vos documents sources ont été préparés pour être intégrés à la base de connaissances.
- Compréhension des exigences de votre modèle d'intégration.

Lors de la configuration des configurations de sécurité, vous pouvez choisir un rôle IAM qui autorise Amazon Bedrock à accéder aux services requis AWS . Vous pouvez laisser Amazon Bedrock créer le rôle de service ou utiliser votre propre rôle personnalisé. Si vous utilisez un rôle personnalisé, configurez une politique de compartiment vectoriel qui limite l'accès au compartiment vectoriel et à l'index vectoriel au rôle personnalisé.

Pour obtenir des informations détaillées sur les autorisations requises et les rôles IAM, consultez la section Créer un rôle de service pour les bases de connaissances Amazon Bedrock dans le guide

de l'utilisateur d'Amazon Bedrock. Le rôle de service doit également disposer d'autorisations pour les vecteurs S3 et les opérations AWS KMS d'API.

Création d'une base de connaissances avec des vecteurs S3

Vous pouvez créer une base de connaissances qui utilise les vecteurs S3 à l'aide de deux méthodes.

Méthode 1 : utilisation de la console Amazon Bedrock

Lorsque vous créez une base de connaissances dans la console Amazon Bedrock, vous pouvez choisir « compartiment vectoriel S3 » comme option de boutique vectorielle. Deux options de configuration s'offrent à vous :

- Création rapide d'un nouveau magasin de vecteurs : Amazon Bedrock crée un compartiment vectoriel S3 et un index vectoriel et les configure avec les paramètres requis pour vous. Par défaut, le compartiment vectoriel est chiffré à l'aide du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Vous pouvez éventuellement chiffrer le compartiment à l'aide AWS KMS de. Pour plus d'informations sur la création rapide d'un nouveau magasin vectoriel dans la console, consultez Créer une base de connaissances en vous connectant à une source de données dans les bases de connaissances Amazon Bedrock du guide de l'utilisateur Amazon Bedrock.
- Choisissez un magasin vectoriel que vous avez créé : choisissez un compartiment vectoriel S3 existant et un index vectoriel provenant de votre compte que vous avez créé précédemment. Pour plus d'informations sur la création d'un bucket vectoriel S3 et d'un index vectoriel dans la console Amazon Bedrock Knowledge Bases, consultez l'onglet S3 Vectors dans Conditions préalables à l'utilisation d'un magasin vectoriel que vous avez créé pour une base de connaissances dans le guide de l'utilisateur d'Amazon Bedrock.

Pour step-by-step obtenir des instructions détaillées, consultez la section Créer une base de connaissances en vous connectant à une source de données dans les bases de connaissances Amazon Bedrock du guide de l'utilisateur d'Amazon Bedrock.

Méthode 2 : utilisation d'Amazon SageMaker Unified Studio

Vous pouvez également créer et gérer des bases de connaissances avec S3 Vectors via Amazon Bedrock dans Amazon SageMaker AI Unified Studio. Cela fournit un environnement de développement unifié pour créer et tester des applications d'IA qui utilisent des bases de connaissances.

Amazon Bedrock in SageMaker AI Unified Studio est conçu pour les utilisateurs qui ont besoin de fonctionnalités de bloc-notes intégrées et qui travaillent sur plusieurs services d' AWS apprentissage automatique et d'analyse. Vous pouvez créer rapidement un compartiment vectoriel S3 et le configurer comme magasin vectoriel pour vos bases de connaissances lorsque vous créez des applications d'IA générative.

Pour plus d'informations sur l'utilisation des vecteurs S3 avec Amazon Bedrock dans SageMaker AI Unified Studio, consultez la section Ajouter une source de données à votre application Amazon Bedrock dans le guide de l'utilisateur d'SageMaker AI Unified Studio.

Gestion et consultation de votre base de connaissances

Synchronisation et gestion des données

Les bases de connaissances Amazon Bedrock proposent des opérations d'ingestion afin de synchroniser vos sources de données et vos intégrations vectorielles. Lorsque vous synchronisez votre source de données, Amazon Bedrock scanne chaque document et vérifie s'il a été indexé dans le magasin vectoriel. Vous pouvez également indexer directement des documents dans le magasin de vecteurs à l'aide de IngestKnowledgeBaseDocumentscette opération. La meilleure pratique consiste à créer un magasin vectoriel distinct pour chaque base de connaissances afin de garantir la synchronisation des données.

Lorsque vous supprimez une base de connaissances ou une ressource de source de données, Amazon Bedrock propose deux politiques de suppression de données : `Delete` (par défaut) et`Retain`. Si vous choisissez cette `Delete` politique, les vecteurs de l'index vectoriel et du compartiment de vecteurs sont automatiquement supprimés.

Interrogation et extraction

Une fois votre base de connaissances configurée, vous pouvez effectuer les opérations suivantes :

- Récupérez des fragments de vos données sources à l'aide de l'opération Retrieve API.
- Générez des réponses basées sur les fragments récupérés à l'aide de l'opération RetrieveAndGenerateAPI.
- Testez les requêtes directement dans la console Amazon Bedrock.

Les réponses sont renvoyées avec des citations des données sources d'origine.

Limites

Lorsque vous utilisez des vecteurs S3 avec les bases de connaissances Amazon Bedrock, vous devez connaître les limites suivantes :

- Recherche sémantique uniquement : S3 Vectors prend en charge la recherche sémantique, mais pas les fonctionnalités de recherche hybrides.
- Limites de taille des vecteurs S3 : Chaque vecteur a une limite de taille totale des métadonnées et une limite de taille pour les métadonnées filtrables, ce qui peut limiter les métadonnées personnalisées et les options de filtrage. Pour plus d'informations sur les métadonnées et les limites de taille des métadonnées filtrables par vecteur, consultezLimites et restrictions.
- Contraintes liées à la stratégie de segmentation : limitée aux modèles qui divisent le contenu en blocs de 500 jetons maximum en raison des restrictions de taille des métadonnées.
- Vecteurs à virgule flottante uniquement : les intégrations de vecteurs binaires ne sont pas prises en charge.

Pour obtenir des conseils complets sur l'utilisation des bases de connaissances Amazon Bedrock, consultez la section Récupérer des données et générer des réponses basées sur l'IA avec les bases de connaissances Amazon Bedrock dans le guide de l'utilisateur d'Amazon Bedrock.

Régions AWS, points de terminaison et quotas pour les vecteurs S3

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Les sections suivantes incluent les AWS régions prises en charge et les quotas de service pour les vecteurs Amazon S3.

AWS Régions et points de terminaison S3 Vectors

Amazon S3 Vectors est actuellement disponible dans les AWS régions suivantes. Pour vous connecter par programmation à un AWS service, vous utilisez un point de terminaison. Pour plus

d'informations sur les points de terminaison de AWS service, consultez la section Points AWS de terminaison de service dans la référence AWS générale. Pour plus d'informations sur les points de terminaison Amazon S3, consultez la section Points de terminaison et quotas Amazon S3 dans le manuel de référence AWS général.

Les points de terminaison S3 Vectors sont des points de terminaison à double pile qui prennent en charge les demandes sur et. IPv6 IPv4

Les points de terminaison VPC Gateway AWS PrivateLink ne sont pas pris en charge.

AWS Régions et points de terminaison S3 Vectors

Nom de la région	Région	Point de terminaison	Protocole	Prise en charge de(s) version(s) de signature
USA Est (Virginie du Nord)	us-east-1	s3vectors.us-east-1.api.aws	HTTPS	4
USA Est (Ohio)	us-east-2	s3vectors.us-east-2.api.aws	HTTPS	4
USA Ouest (Orego	us-west-2	s3vectors.us-west-2.api.aws	HTTPS	4
EU Centra 1 (Franc t)	eu-central-1	s3vectors.eu-central-1.api.aws	HTTPS	4
Asie-Paci	ap-southeast-2	s3vectors.ap-southeast-2.api.aws	HTTPS	4

Nom de la région	Région	Point de terminaison	Protocole	Prise en charge de(s) version(s) de signature
fique (Sydne				

Quotas de service S3 Vectors

Les quotas, également appelés limites, sont le nombre maximum de ressources de service ou d'opérations pour votre AWS compte. Les limites sont les quotas de service pour les ressources S3 Vectors.

Pour connaître les limites détaillées qui s'appliquent aux vecteurs S3, consultezLimites et restrictions.

Sauf indication contraire, chaque quota est établi par AWS région. Vous pouvez demander des augmentations pour certains quotas, tandis que d'autres quotas ne peuvent pas être augmentés. Pour plus d'informations sur la demande d'augmentation de quota, consultez la section Demander une augmentation de quota dans le Guide de l'utilisateur du Service Quotas. Pour plus d'informations sur les quotas Amazon S3, consultez la section Points de terminaison et quotas Amazon S3 dans le manuel de référence AWS général.

La sécurité dans les vecteurs S3

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Amazon S3 Vectors propose un stockage vectoriel extrêmement durable. Les données écrites dans S3 Vectors sont stockées sur S3, qui est conçu pour garantir une durabilité des données de 99,999999999 % (11 neuf).

S3 Vectors met en œuvre une approche de sécurité qui inclut le chiffrement au repos et la transmission sécurisée des données. Que vous stockiez des millions de vecteurs pour des applications d'apprentissage automatique ou que vous développiez des systèmes de recherche

sémantiques, S3 Vectors fournit les contrôles de sécurité nécessaires pour répondre aux exigences de conformité et de protection des données de votre entreprise.

Rubriques

- Gestion des identités et des accès dans S3 Vectors
- Protection des données et chiffrement dans S3 Vectors

Gestion des identités et des accès dans S3 Vectors

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

La gestion des accès dans S3 Vectors suit les meilleures pratiques en matière de AWS sécurité, en fournissant plusieurs niveaux de contrôle pour garantir que seuls les utilisateurs et les applications autorisés peuvent accéder à vos données vectorielles. Le service s'intègre à IAM et prend en charge les politiques basées sur les identités et les ressources, ce qui vous donne de la flexibilité dans la manière dont vous structurez et gérez les autorisations au sein de votre organisation.

Authentification et autorisation des demandes

S3 Vectors utilise des mécanismes d'authentification et d'autorisation AWS standard pour sécuriser l'accès aux compartiments vectoriels et à leur contenu. Chaque demande adressée à S3 Vectors doit être authentifiée à l'aide AWS d'informations d'identification valides, et le service évalue les autorisations en fonction de la combinaison de politiques basées sur l'identité, de politiques basées sur les ressources et de toute politique de contrôle de service applicable.

Le processus d'authentification commence lorsqu'un client adresse une demande à S3 Vectors à l'aide AWS d'informations d'identification (clés d'accès, informations d' AWS STS identification temporaires ou rôles IAM). Le service valide ces informations d'identification, puis évalue les autorisations associées à l'identité authentifiée par rapport à l'action demandée et à la ressource cible. Ce processus d'évaluation prend en compte plusieurs types de politiques et applique le principe du moindre privilège pour déterminer si la demande doit être autorisée ou refusée.

L'autorisation dans S3 Vectors fonctionne à plusieurs niveaux de granularité. Vous pouvez contrôler l'accès au niveau du compartiment vectoriel, au niveau de l'index vectoriel individuel ou même des

opérations spécifiques au sein d'un index. Ce modèle d'autorisation hiérarchique vous permet de mettre en œuvre des schémas de contrôle d'accès sophistiqués qui correspondent à votre structure organisationnelle et aux exigences de gouvernance des données.

Types de ressources définis pour les compartiments vectoriels

S3 Vectors définit des types de ressources spécifiques qui peuvent être référencés dans les politiques IAM et les politiques basées sur les ressources. Il est essentiel de comprendre ces types de ressources pour créer des politiques de contrôle d'accès efficaces qui fournissent le niveau d'accès approprié aux utilisateurs et aux applications appropriés.

Le tableau suivant décrit les types de ressources disponibles dans S3 Vectors.

Types de ressources disponibles dans S3 Vectors

Type de ressource	Format ARN	Description
VectorBucket	arn:aws:s3vector : ::bucket/ *region 123456789012 bucket-name*	Représente un bucket vectoriel et est utilisé pour les opérations au niveau du bucket telles que la création, la suppression ou la configura tion du bucket
Index	arn:aws:s3vector : ::bucket/ / index/ *region 123456789 012 bucket-name index-name*	Représente un index vectoriel dans un compartiment et est utilisé pour des opérations spécifiques à l'index, telles que l'interrogation de vecteurs ou la gestion du contenu de l'index

Actions politiques pour les seaux vectoriels

S3 Vectors fournit un ensemble complet d'actions politiques correspondant aux différentes opérations que vous pouvez effectuer sur les buckets et les index vectoriels. Ces actions sont conçues pour fournir un contrôle précis sur les personnes habilitées à effectuer des opérations spécifiques, vous permettant ainsi de mettre en œuvre efficacement le principe du moindre privilège.

Le tableau suivant répertorie toutes les actions politiques disponibles pour les ressources S3 Vectors.

Actions politiques pour les ressources S3 Vectors

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
Compte	ListVectorBuckets	vecteurs S3 : ListVectorBuckets	Permet de répertorier tous les compartiments vectoriels du compte et de la région	Liste	
VectorBucket	CreateVectorBucket	vecteurs S3 : CreateVectorBucket	Accorde l'autorisation de créer un nouveau compartiment vectoriel avec une configuration spécifiée	Écrire	Vecteurs S3 : SSEType, vecteurs S3 : kmsKeyArn
VectorBucket	GetVectorBucket	vecteurs S3 : GetVectorBucket	Accorde l'autorisation de récupérer les attributs et la configuration du compartiment vectoriel	Lecture	
VectorBucket	DeleteVectorBucket	vecteurs S3 : DeleteVectorBucket	Autorise la suppression d'un	Écrire	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
			compartiment vectoriel vide		
VectorBucket	ListIndexes	vecteurs S3 : ListIndexes	Permet de répertorier tous les index d'un bucket vectoriel	Liste	
VectorBucket	PutVector BucketPolicy	vecteurs S3 : PutVector BucketPolicy	Accorde l'autorisation d'appliquer ou de mettre à jour une politique basée sur les ressources sur un bucket vectoriel	Gestion des autorisations	
VectorBucket	GetVector BucketPolicy	vecteurs S3 : GetVector BucketPolicy	Accorde l'autorisation de récupérer la politique basée sur les ressource s attachée à un bucket vectoriel	Lecture	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
VectorBucket	DeleteVectorBucketPolicy	vecteurs S3 : DeleteVectorBucketPolicy	Accorde l'autorisation de supprimer la politique basée sur les ressources d'un bucket vectoriel	Gestion des autorisations	
Index	CreateIndex	vecteurs S3 : CreateIndex	Autorise la création d'un nouvel index vectoriel avec des dimensions et une configuration de métadonnées spécifiées	Écrire	
Index	GetIndex	vecteurs S3 : GetIndex	Accorde l'autorisation de récupérer les attributs et la configuration de l'index vectoriel	Lecture	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
Index	DeleteIndex	vecteurs S3 : DeleteIndex	Autorise la suppression d'un index vectoriel et de tout son contenu	Écrire	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
Index	QueryVectors	Vecteurs S3 (obligatoires) : QueryVectors	Accorde l'autorisation d'effectuer des requêtes de similarité par rapport aux vecteurs d'un index. Avec **`s3vectors:QueryVectors`** Only, vous pouvez récupérer les clés vectorielles des voisins les plus proches approximatifs et leurs distances calculées à partir du vecteur de requête. Cette autorisation est suffisante uniquement lorsque vous ne définissez aucun	Lecture	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
			filtre de métadonnées et que vous ne demandez pas de données vectoriel les ou de métadonné es (en maintenant le `returnMetadata` paramètre défini sur false ou non spécifié).		

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
		(Conditionnellement requis) : s3vector : GetVectors	Obligatoire si vous définissez des filtres de métadonnées, définis `returnMetadata` sur true dans votre demande. Avec les deux **`s3vectors:QueryVectors`** options et **`s3vectors:GetVectors`** , vous pouvez filtrer les résultats en utilisant des critères de métadonnées et récupérer les clés vectoriel les ainsi que leurs données	Lecture	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
			associées , leurs métadonnées et les distances calculées par rapport au vecteur de requête.		
Index	PutVectors	vecteurs S3 : PutVectors	Autorise l'ajout ou la mise à jour de vecteurs dans un index	Écrire	
Index	GetVectors	vecteurs S3 : GetVectors	Autorise la récupération de vecteurs spécifiques et de leurs métadonnées par clé vectorielle	Lecture	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
Index	ListVectors	Vecteurs S3 (obligatoires) : ListVectors	Accorde l'autorisation de répertorier les clés vectoriel les dans un index. Avec **`s3vectors:ListVectors`** Only, vous pouvez répertorier les clés vectoriel les lorsque `returnData` les deux `returnMetadata` paramètres sont faux ou non spécifiés.	Lecture	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
		(Conditionnellement requis) : s3vector : GetVectors	Obligatoire si vous définissez l'`returnData` un ou l'autre des `returnMetadata` paramètres sur true dans votre demande. Avec les deux **`s3vectors:ListVectors`** options et **`s3vectors:GetVectors`** , vous pouvez récupérer les clés vectorielles ainsi que leurs données et métadonnées associées en réglant `returnData` et en	Lecture	

Type de ressource	Opérations d'API	Actions de politique	Description des actions de politique	Niveau d'accès	Clés de condition
			réglant `returnMetadata` sur true.		
Index	DeleteVectors	vecteurs S3 : DeleteVectors	Autorise la suppression de vecteurs spécifiques d'un index	Écrire	

Ces actions peuvent être combinées de différentes manières pour créer des politiques qui répondent à vos besoins d'accès spécifiques. Par exemple, vous pouvez créer une politique en lecture seule qui inclut`s3vectors:GetVectorBucket`,, et des `s3vectors:GetVectors` actions `s3vectors:ListIndexes``s3vectors:QueryVectors`, ou une politique qui inclut des autorisations de requête et de récupération vectorielle mais exclut les actions administratives telles que la création ou la suppression d'index.

Clés de condition pour les seaux vectoriels

Clés de condition pour les seaux vectoriels

	Clés de condition	Description	Type
1	Vecteurs S3 : SSEType	Filtre l'accès par type de chiffrement côté serveur Valeurs valides : `AES256` | `aws:kms`	Chaîne
2	vecteurs S3 : kmsKeyArn	Filtre l'accès par l' AWS AWS KMS ARN de la clé utilisée pour	ARN

	Clés de condition	Description	Type
		chiffrer un bucket vectoriel	

Exemples de politiques basées sur l'identité de S3 Vectors

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Les politiques basées sur l'identité IAM sont des documents JSON que vous attachez aux utilisateurs, groupes ou rôles IAM pour définir les actions qu'ils peuvent effectuer sur les ressources S3 Vectors. Ces politiques sont évaluées dans le contexte de l'identité à l'origine de la demande et fournissent un moyen centralisé de gérer les autorisations dans votre AWS environnement. Les politiques basées sur l'identité fournissent une piste d'audit claire permettant de déterminer qui dispose de quelles autorisations et peuvent être facilement modifiées en fonction de l'évolution de vos besoins en matière d'accès.

Lorsque vous concevez des politiques basées sur l'identité pour les vecteurs S3, tenez compte des différents types d'utilisateurs et d'applications qui interagiront avec vos données vectorielles. Les modèles courants incluent les data scientists qui ont besoin d'interroger des vecteurs, les ingénieurs de données qui ont besoin de charger et de gérer des données vectorielles, les administrateurs qui ont besoin d'un contrôle total sur la configuration des compartiments et les applications qui ont besoin d'un accès spécifique en lecture ou en écriture à des index vectoriels spécifiques.

Exemples de politiques

Politique d'accès administratif

Cette politique fournit un accès administratif complet aux ressources S3 Vectors, adaptées aux administrateurs de plateformes ou aux DevOps équipes :

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

```
            "Sid": "AllowAdministrativeAccess",
            "Effect": "Allow",
            "Action": [
                "s3vectors:CreateVectorBucket",
                "s3vectors:PutVectorBucketPolicy",
                "s3vectors:DeleteVectorBucket",
                "s3vectors:DeleteVectorBucketPolicy",
                "s3vectors:GetVectorBucket",
                "s3vectors:GetVectorBucketPolicy",
                "s3vectors:ListVectorBuckets",
                "s3vectors:CreateIndex",
                "s3vectors:DeleteIndex",
                "s3vectors:GetIndex",
                "s3vectors:ListIndexes",
                "s3vectors:DeleteVectors",
                "s3vectors:GetVectors",
                "s3vectors:ListVectors",
                "s3vectors:PutVectors",
                "s3vectors:QueryVectors"
            ],
            "Resource": "*"
        }
    ]
}
```

Politique d'accès spécifique à l'application

Cette politique est conçue pour les applications qui doivent effectuer des opérations spécifiques sur des index vectoriels désignés :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowApplicationVectorAccess",
            "Effect": "Allow",
            "Action": [
                "s3vectors:QueryVectors",
                "s3vectors:GetVectors",
                "s3vectors:PutVectors",
                "s3vectors:ListVectors"
            ],
            "Resource": [
```

```
                "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-vector-
bucket/index/product-recommendations",
                "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-vector-
bucket/index/content-similarity"
            ]
        },
        {
            "Sid": "AllowGetIndex",
            "Effect": "Allow",
            "Action": "s3vectors:GetIndex",
            "Resource": "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-
vector-bucket/index/*"
        },
        {
            "Sid": "AllowIndexInspection",
            "Effect": "Allow",
            "Action": "s3vectors:ListIndexes",
            "Resource": "arn:aws:s3vectors:aws-region:123456789012:bucket/amzn-s3-demo-
vector-bucket"
        }
    ]
}
```

Exemples de politiques basées sur les ressources S3 Vectors

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Les politiques basées sur les ressources sont attachées à une ressource. Vous pouvez créer des politiques basées sur les ressources pour les compartiments vectoriels. Les politiques basées sur les ressources pour les vecteurs S3 utilisent le format de AWS politique standard en JSON que vous attachez directement aux compartiments vectoriels pour contrôler l'accès au compartiment et à son contenu.

Contrairement aux politiques basées sur l'identité associées aux utilisateurs, aux groupes ou aux rôles, les politiques basées sur les ressources sont associées à la ressource elle-même (le compartiment vectoriel) et peuvent accorder des autorisations aux principaux depuis d'autres comptes. AWS Ils sont donc idéaux pour les scénarios dans lesquels vous devez partager des

données vectorielles au-delà des limites de l'organisation ou mettre en œuvre des contrôles d'accès précis en fonction de la ressource spécifique à laquelle vous accédez.

Les politiques basées sur les ressources sont évaluées en combinaison avec les politiques basées sur l'identité, et les autorisations effectives sont déterminées par l'union de toutes les politiques applicables. Cela signifie qu'un principal doit obtenir l'autorisation de la part de la politique basée sur l'identité (attachée à son utilisateur/rôle) et de la politique basée sur les ressources (attachée au compartiment) pour effectuer une action, sauf si la politique basée sur les ressources accorde explicitement l'autorisation.

Exemple 1 : politique d'accès entre comptes

Cette politique explique comment accorder des autorisations spécifiques aux utilisateurs de différents AWS comptes :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CrossAccountBucketAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam:123456789012:role/Admin"
            },
            "Action": [
                "s3vectors:CreateIndex",
                "s3vectors:ListIndexes",
                "s3vectors:QueryVectors",
                "s3vectors:PutVectors",
                "s3vectors:DeleteIndex"
            ],
            "Resource": [
                "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket/*",
                "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket"
            ]
        }
    ]
}
```

Exemple 2 : Refuser les actions au niveau de l'index vectoriel

Cette politique explique comment refuser des actions spécifiques au niveau de l'index vectoriel à un rôle IAM :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyIndexLevelActions",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam:123456789012:role/External-Role-Name"
            },
            "Action": [
                "s3vectors:QueryVectors",
                "s3vectors:PutVectors",
                "s3vectors:DeleteIndex",
                "s3vectors:GetVectors",
                "s3vectors:GetIndex",
                "s3vectors:DeleteVectors",
                "s3vectors:CreateIndex",
                "s3vectors:ListVectors"
            ],
            "Resource": "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-bucket/*"
        }
    ]
}
```

Exemple 3 : Refuser les opérations de modification à la fois au niveau de l'index vectoriel et au niveau du bucket

Cette politique explique comment refuser les demandes de modification pour les actions d'index vectoriel et de niveau bucket en spécifiant plusieurs ressources :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyModificationActionsAtBucketandIndexLevels",
            "Effect": "Deny",
```

```
            "Principal": {
                "AWS": "arn:aws:iam:123456789012:role/External-Role-Name"
            },
            "Action": [
                "s3vectors:CreateVectorBucket",
                "s3vectors:DeleteVectorBucket",
                "s3vectors:PutVectorBucketPolicy",
                "s3vectors:DeleteVectorBucketPolicy",
                "s3vectors:CreateIndex",
                "s3vectors:DeleteIndex",
                "s3vectors:PutVectors",
                "s3vectors:DeleteVectors"
            ],
            "Resource": [
                "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-
bucket/*",
                "arn:aws:s3vectors:aws-region:111122223333:bucket/amzn-s3-demo-vector-
bucket"
            ]
        }
    ]
}
```

Protection des données et chiffrement dans S3 Vectors

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Amazon S3 Vectors assure une durabilité de 99,999999999 % (11 9 s) pour vos données vectorielles, ce qui garantit une fiabilité exceptionnelle pour vos besoins de stockage vectoriel. Cette durabilité est soutenue par l'infrastructure éprouvée d'Amazon S3, conçue pour préserver l'intégrité et la disponibilité des données, même en cas de panne matérielle ou d'autres perturbations.

La protection des données dans S3 Vectors comprend plusieurs niveaux de contrôles de sécurité conçus pour protéger vos données vectorielles au repos et en transit.

Par défaut, tous les nouveaux vecteurs contenus dans les compartiments vectoriels Amazon S3 Vectors utilisent le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Lorsque

vous créez un compartiment vectoriel avec un chiffrement SSE-S3, toutes les opérations suivantes sur le compartiment utilisent automatiquement le chiffrement.

S3 Vectors s'intègre également au service de gestion des AWS clés (KMS) pour fournir des options flexibles de gestion des clés de chiffrement, vous permettant de choisir des clés gérées par le client pour le contrôle des autorisations et l'auditabilité.

Configuration du comportement de chiffrement côté serveur pour les compartiments vectoriels Amazon S3

La configuration du chiffrement dans S3 Vectors est un paramètre de sécurité fondamental à spécifier lorsque vous créez un compartiment vectoriel. Cette conception garantit que toutes les données vectorielles stockées dans le compartiment sont cryptées dès leur création. La configuration de chiffrement s'applique à tous les vecteurs, index vectoriels et métadonnées du compartiment, offrant ainsi une protection cohérente sur l'ensemble de votre jeu de données vectorielles dans un compartiment vectoriel.

> **Important**
>
> Les paramètres de chiffrement d'un compartiment vectoriel ne peuvent pas être modifiés une fois le compartiment vectoriel créé. Vous devez examiner attentivement vos exigences en matière de chiffrement lors du processus de création du compartiment, notamment les exigences de conformité, les préférences en matière de gestion des clés et l'intégration à l'infrastructure de sécurité existante.

Le type de chiffrement SSE-S3 ou SSE-KMS est défini au niveau du compartiment vectoriel et s'applique à tous les index vectoriels et vecteurs du compartiment. Vous ne pouvez pas modifier les paramètres de chiffrement pour les index individuels d'un bucket. La configuration de chiffrement s'applique non seulement aux données vectorielles elles-mêmes, mais également à toutes les métadonnées associées.

Utilisation du chiffrement SSE-S3

Le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) fournit une solution de chiffrement simple et efficace pour les compartiments vectoriels qui AWS gère tous les aspects du processus de chiffrement. Cette méthode de chiffrement utilise `AES-256` le chiffrement et est conçue pour fournir une sécurité renforcée avec une charge opérationnelle minimale, fournissant

aux entreprises un chiffrement robuste sans la complexité des besoins liés à la gestion des clés de chiffrement.

Avec SSE-S3, Amazon S3 gère automatiquement la génération, la rotation et la gestion des clés de chiffrement. Le SSE-S3 fournit une sécurité renforcée sans configuration supplémentaire ni exigences de gestion continue. Les processus de chiffrement et de déchiffrement sont gérés automatiquement par le service, et l'utilisation du chiffrement SSE-S3 n'entraîne aucun frais supplémentaire au-delà de la tarification standard de S3 Vectors.

Utilisation du chiffrement SSE-KMS

Le chiffrement côté serveur à l'aide des AWS clés du service de gestion des clés (SSE-KMS) permet de mieux contrôler les clés de chiffrement et de consigner des audits détaillés sur l'utilisation des clés. Cette méthode de chiffrement est idéale pour les entreprises soumises à des exigences de conformité strictes, celles qui doivent mettre en œuvre des politiques personnalisées de rotation des clés ou les environnements dans lesquels des pistes d'audit détaillées de l'accès aux données sont requises.

SSE-KMS vous permet d'utiliser des clés gérées par le client (CMKs) pour chiffrer vos données vectorielles. Les clés gérées par le client offrent le plus haut niveau de contrôle, vous permettant de définir des politiques clés, d'activer ou de désactiver les clés et de surveiller l'utilisation des clés de bout en bout AWS CloudTrail. Ce niveau de contrôle rend le SSE-KMS particulièrement adapté aux industries réglementées ou aux organisations ayant des exigences spécifiques en matière de gouvernance des données.

Lorsque vous utilisez SSE-KMS avec des clés gérées par le client, vous avez un contrôle total sur les personnes autorisées à utiliser les clés pour chiffrer et déchiffrer les données. Vous pouvez créer des politiques clés détaillées qui spécifient quels utilisateurs, rôles ou services peuvent accéder aux clés.

Considérations importantes pour le SSE-KMS

- Exigences relatives au format des clés KMS : S3 Vectors nécessite que vous spécifiiez les clés KMS en utilisant le format Amazon Resource Name (ARN) complet. Les clés IDs ou les alias de clé ne sont pas pris en charge.
- Autorisations principales du service : Lorsque vous utilisez des clés gérées par le client avec S3 Vectors, vous devez explicitement accorder des autorisations au principal du service S3 Vectors pour qu'il utilise votre clé KMS. Cette exigence garantit que le service peut chiffrer et déchiffrer vos données en votre nom. Le principal de service qui nécessite un accès est `indexing.s3vectors.amazonaws.com`.

Exemple : politique de clé KMS pour les vecteurs S3

Pour utiliser une clé KMS gérée par le client avec S3 Vectors, vous devez mettre à jour votre politique en matière de clés afin d'inclure des autorisations pour le principal du service S3 Vectors. Voici un exemple de politique clé complet.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowS3VectorsServicePrincipal",
            "Effect": "Allow",
            "Principal": {
                "Service": "indexing.s3vectors.amazonaws.com"
            },
            "Action": "kms:Decrypt",
            "Resource": "*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3vectors:aws-region:123456789012:bucket/
*"
                },
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ForAnyValue:StringEquals": {
                    "kms:EncryptionContextKeys": ["aws:s3vectors:arn",
 "aws:s3vectors:resource-id"]
                }
            }
        },
        {
            "Sid": "AllowApplicationAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam:123456789012:role/VectorApplicationRole",
                    "arn:aws:iam:123456789012:user/DataScientist"
                ]
            },
            "Action": [
                "kms:Decrypt",
```

```
                "kms:GenerateDataKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "s3vectors.aws-region.amazonaws.com"
                },
                "ForAnyValue:StringEquals": {
                    "kms:EncryptionContextKeys": ["aws:s3vectors:arn",
 "aws:s3vectors:resource-id"]
                }
            }
        }
    ]
}
```

- Autorisations KMS requises :
  - Autorisation principale du service S3 Vectors :
    - `kms:Decrypt`— Requis par le responsable du service S3 Vectors (`indexing.s3vectors.amazonaws.com`) sur votre clé gérée par le client pour maintenir et optimiser l'index lors des opérations en arrière-plan
  - Autorisations principales de l'IAM :
    - `kms:Decrypt`— Nécessaire pour toutes les opérations au niveau vectoriel (PutVectors,, GetVectorsQueryVectors, DeleteVectors) ListVectors
    - `kms:GenerateDataKey`— Nécessaire pour créer un bucket vectoriel à l'aide de la clé gérée par le client
- Considérations relatives à l'accès entre comptes : Lorsque vous implémentez des modèles d'accès entre comptes avec SSE-KMS, vous devez vous assurer que la politique des clés KMS autorise l'accès depuis les principaux appropriés aux autres comptes. Le format ARN de la clé devient particulièrement important dans les scénarios entre comptes, car il fournit une référence claire à la clé quel que soit le contexte du compte à partir duquel on y accède.

Configuration du chiffrement dans les vecteurs S3

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Cette rubrique explique comment afficher la configuration de chiffrement de vos compartiments vectoriels S3.

Avant de commencer, assurez-vous que vous disposez des éléments suivants :

- Un compartiment vectoriel S3 avec chiffrement configuré.
- Autorisations appropriées pour consulter les propriétés du bucket.

Utilisation de la console S3

Pour configurer le chiffrement d'un compartiment vectoriel

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Vector buckets.
3. Choisissez Create vector bucket.
4. Pour Nom du compartiment, saisissez le nom de votre compartiment.

   Le nom du compartiment doit présenter les caractéristiques suivantes :

   - Soyez unique dans votre compte pour cette AWS région
   - Il doit comporter entre 3 et 63 caractères.
   - Composé uniquement de lettres minuscules, de chiffres et de traits d'union (-)
5. Pour le chiffrement, choisissez l'une des options suivantes :

   - Ne spécifiez pas le type de chiffrement : Amazon S3 applique le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de chiffrement de base pour les nouveaux objets.
   - Spécifier le type de cryptage : choisissez une méthode de cryptage spécifique :

- Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) : Amazon S3 chiffre vos données au niveau de l'objet lorsqu'il les écrit sur des disques et les déchiffre lorsque vous y accédez.
- Chiffrement côté serveur avec AWS clés du service de gestion des clés (SSE-KMS) : similaire au SSE-S3, mais utilise des clés gérées par le client (CMKs) dans AWS KMS, ce qui vous permet de mieux contrôler vos clés. Pour plus d'informations sur les clés gérées par le client, consultez la section Clés gérées par le client dans le Guide du développeur du service de gestion des AWS clés.

  Si vous sélectionnez cette option, sous cléAWS KMS, choisissez l'une des options suivantes :

  - Choisissez parmi vos clés AWS KMS — Sélectionnez une clé KMS existante dans la liste déroulante
  - Entrez l'ARN de la clé AWS KMS — Entrez le nom de ressource Amazon (ARN) d'une clé KMS
  - Création d'une clé KMS : créez une nouvelle clé gérée par le client dans la console AWS KMS. Pour plus d'informations, consultez la section Création de clés symétriques gérées par le client dans le Guide du développeur du service de gestion des AWS clés.

> **Note**
>
> Les exigences suivantes s'appliquent à la clé KMS :
>
> - AWS L'ID de clé KMS ne doit pas être vide
> - Votre clé KMS doit se trouver dans la même région que celle dans laquelle ce compartiment est créé
> - AWS L'ARN de la clé KMS doit commencer par « arn:aws:kms : »

> **Important**
>
> Les paramètres de chiffrement ne peuvent pas être modifiés une fois le bucket vectoriel créé.

6. Si vous avez choisi Enter AWS KMS key ARN, saisissez l'ARN dans le champ de texte prévu à cet effet.

7. Si vous avez choisi Créer une clé KMS, la console ouvre la console AWS KMS dans un nouvel onglet. Pour obtenir des instructions sur la création d'une clé KMS, voir Création de clés symétriques gérées par le client dans le Guide du développeur du service de gestion des AWS clés.
8. Choisissez Create vector bucket.

> **Important**
>
> Lorsque vous utilisez le chiffrement KMS, assurez-vous que les principaux IAM qui ont besoin d'accéder aux objets du compartiment disposent de l'autorisation KMS nécessaire (KMS:Decrypt) pour la clé KMS sélectionnée.

À l'aide du AWS CLI

L'exemple suivant montre comment créer un compartiment vectoriel avec la configuration de chiffrement SSE-S3 à l'aide du. AWS CLI Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3vectors create-vector-bucket \
        --vector-bucket-name "amzn-s3-demo-vector-bucket" \
        --encryption-configuration '{"sseType": "AES256"}'
```

Les exemples suivants montrent comment créer un compartiment vectoriel qui utilise la configuration de chiffrement SSE-KMS avec une clé gérée par le client. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3vectors create-vector-bucket \
        --vector-bucket-name "amzn-s3-demo-vector-bucket" \
        --encryption-configuration '{"sseType": "aws:kms", "kmsKeyArn":
 "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"}'
```

Affichage de la configuration de chiffrement dans S3 Vectors

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Après avoir créé votre bucket vectoriel, vous pouvez vérifier la configuration du chiffrement à l'aide de la console ou de la CLI.

En utilisant le AWS CLI

Utilisez la `get-vector-bucket` commande pour récupérer des informations détaillées sur le compartiment, notamment la configuration du chiffrement. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3vectors get-vector-bucket \
  --vector-bucket-name amzn-s3-demo-vector-bucket
```

Journalisation avec AWS CloudTrail for S3 Vectors

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Amazon S3 Vectors est intégré à AWS 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 vecteurs S3 sous forme d'événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à S3 Vectors, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires. Lorsqu'une activité événementielle prise en charge se produit dans S3 Vectors, cette activité est enregistrée dans un CloudTrail événement. Vous pouvez utiliser le journal CloudTrail pour enregistrer les événements de gestion et les événements de données pour les vecteurs S3.

Pour en savoir plus CloudTrail, consultez le guide de CloudTrail l'utilisateur.

Informations sur les vecteurs S3 dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité se produit dans S3 Vectors, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements de AWS service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris les événements liés aux vecteurs S3, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un journal de suivi dans la console, il s'applique à toutes les régions AWS . Le journal enregistre les événements de toutes les régions de la AWS partition et transmet les fichiers journaux au compartiment Amazon S3 que vous spécifiez. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez la section Présentation de la création d'un journal, de la configuration des notifications Amazon SNS pour CloudTrail, de la réception de fichiers CloudTrail journaux provenant de plusieurs régions et de la réception de fichiers CloudTrail journaux de plusieurs comptes dans le guide de l'CloudTrailutilisateur.

Toutes les actions de l'API S3 Vectors sont enregistrées CloudTrail et documentées dans le manuel Amazon S3 Vectors API Reference. Par exemple, les appels aux CreateVectorBucketCreateIndex, et QueryVectorsles actions génèrent des entrées dans les fichiers CloudTrail journaux.

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 les éléments suivants :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou IAM.
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré.
- Si la demande a été faite par un autre AWS service.

Pour en savoir plus, consultez Élément userIdentity CloudTrail dans le Guide de l'utilisateur CloudTrail .

CloudTrail événements de gestion pour S3 Vectors

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre AWS compte. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

Pour les vecteurs S3, CloudTrail enregistre les événements de gestion suivants :

- CreateVectorBucket
- DeleteVectorBucket
- GetVectorBucket

- ListVectorBuckets
- PutVectorBucketPolicy
- GetVectorBucketPolicy
- DeleteVectorBucketPolicy
- CreateIndex
- DeleteIndex
- GetIndex
- ListIndexes

`eventSource`Pour S3 Vectors, les événements de gestion et les événements de données sont`s3vectors.amazonaws.com`.

Pour plus d'informations sur les événements de gestion, consultez la section Journalisation des événements de gestion dans le Guide de CloudTrail l'utilisateur.

CloudTrail événements de données pour les vecteurs S3

Les événements de données fournissent des informations sur les opérations de ressource exécutées sur ou dans une ressource. Ils sont également connus sous le nom opérations de plans de données. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. Cependant, vous pouvez configurer des sentiers pour consigner les événements de données pour les ressources S3 Vectors.

Lorsque vous configurez votre journal pour consigner les événements liés aux données, vous pouvez spécifier le type de ressource S3 Vectors. S3 Vectors prend en charge les types de ressources suivants pour les événements de données :

- `AWS::S3Vectors::VectorBucket`- Enregistre les événements de données pour tous les index vectoriels contenus dans les compartiments vectoriels spécifiés
- `AWS::S3Vectors::Index`- Enregistre les événements de données pour des index vectoriels spécifiques

Pour les vecteurs S3, CloudTrail enregistre les événements de données suivants :

Opérations sur les données vectorielles :

- PutVectors- Enregistre lorsque des vecteurs sont ajoutés à un index vectoriel
- GetVectors- Enregistre les cas où des vecteurs sont récupérés à partir d'un index vectoriel

- DeleteVectors- Enregistre les cas où des vecteurs sont supprimés d'un index vectoriel
- ListVectors- Enregistre les cas où les vecteurs d'un index vectoriel sont listés
- QueryVectors- Enregistre lorsque des requêtes de similarité sont effectuées sur un index vectoriel

`eventSource`Pour les événements de données S3 Vectors, c'est`s3vectors.amazonaws.com`.

Activation de la journalisation des événements de données pour les vecteurs S3

Vous pouvez activer la journalisation des événements de données pour les ressources S3 Vectors lorsque vous créez ou mettez à jour un CloudTrail suivi. Vous pouvez spécifier la journalisation pour tous les compartiments vectoriels et index vectoriels de votre compte, ou vous pouvez spécifier des compartiments vectoriels ou des index vectoriels individuels. Pour connaître les étapes détaillées relatives à la création d'un parcours, reportez-vous à la section Création d'un parcours dans le guide de CloudTrail l'utilisateur.

Pour activer la journalisation des événements de données pour toutes les ressources S3 Vectors :

- Lors de la création ou de la mise à jour d'un suivi, choisissez Data events.
- Pour Type de ressource, sélectionnez`AWS::S3Vectors::VectorBucket`.
- Pour Resource ARN, entrez `arn:aws:s3vectors:_:_:bucket/*` pour enregistrer les événements pour tous les compartiments vectoriels ou spécifiez un compartiment vectoriel individuel ARNs (par exemple,`arn:aws:s3vectors:`*`us-east-1`*`:`*`123456789012`*`:bucket/`*`amzn-s3-demo-vector-bucket`*).

Pour activer la journalisation des événements de données pour des index vectoriels spécifiques, procédez comme suit :

- Lors de la création ou de la mise à jour d'un suivi, choisissez Data events.
- Pour Type de ressource, sélectionnez`AWS::S3Vectors::Index`.
- Pour Resource ARN, entrez l'ARN de l'index vectoriel spécifique, tel que :`arn:aws:s3vectors:`*`us-east-1`*`:`*`123456789012`*`:bucket/`*`amzn-s3-demo-vector-bucket`*`/index/`*`my-index`*.

Pour plus d'informations sur les événements liés aux données, consultez la section Enregistrement des événements liés aux données dans le Guide de CloudTrail l'utilisateur.

Rubriques

- CloudTrail exemple de fichier journal pour les vecteurs S3

CloudTrail exemple de fichier journal pour les vecteurs S3

> **Note**
>
> Amazon S3 Vectors est en version préliminaire pour Amazon Simple Storage Service et est sujet à modification.

Les exemples suivants présentent des entrées de CloudTrail journal pour les événements de données S3 Vectors. Les événements de données sont enregistrés lorsque vous effectuez des opérations sur des données vectorielles dans vos index vectoriels.

Exemple : fichier CloudTrail journal pour un événement **`GetVectors`** de données


```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:user/myUserName",
        "accountId": "123456789012",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
    },
    "eventTime": "2024-11-22T17:12:25Z",
    "eventSource": "s3vectors.amazonaws.com",
    "eventName": "GetVectors",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "[aws-cli/2.18.5]",
    "requestParameters": {
        "vectorBucketName": "amzn-s3-demo-vector-bucket",
        "returnMetadata": "false",
        "indexName": "111aa1111-22bb-33cc-44dd-5555eee66ffff",
        "returnData": "false"
    },
    "responseElements": null,
    "additionalEventData": {
```

```
        "SignatureVersion": "SigV4",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256"
    },
    "requestID": "07D681123BD12AED",
    "eventID": "f2b287f3-0df1-1234-a2f4-c4bdfed47657",
    "readOnly": true,
    "resources": [{
        "accountId": "123456789012",
        "type": "AWS::S3Vectors::VectorBucket",
        "ARN": "arn:aws:s3vectors:us-east-1:123456789012:bucket/amzn-s3-demo-vector-
bucket"
    }, {
        "accountId": "123456789012",
        "type": "AWS::S3Vectors::Index",
        "ARN": "arn:aws:s3vectors:us-east-1:123456789012:bucket/amzn-s3-demo-vector-
bucket/index/111aa1111-22bb-33cc-44dd-5555eee66ffff"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": false,
    "recipientAccountId": "444455556666",
    "eventCategory": "Data",
    "tlsDetails": {
        "tlsVersion": "TLSv1.2",
        "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
        "clientProvidedHostHeader": "client-host"
    }
}
```


Comprendre les entrées du fichier journal des vecteurs S3

CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

Les entrées du CloudTrail journal S3 Vectors contiennent les éléments clés suivants :

- EventSource - Toujours `s3vectors.amazonaws.com` pour les événements S3 Vectors.
- EventName - L'opération d'API S3 Vectors qui a été effectuée.
- EventCategory : soit `Management` pour les opérations du plan de contrôle, soit `Data` pour les opérations du plan de données.

- ReadOnly : `true` pour les opérations de lecture (par exemple GetVectors, QueryVectors, ListVectors) et `false` pour les opérations d'écriture (PutVectors, DeleteVectors).
- ressources - Les ressources S3 Vectors impliquées dans l'opération, y compris les buckets vectoriels et les index vectoriels.
- RequestParameters : paramètres envoyés avec la demande.
- ResponseElements : éléments de réponse renvoyés par le service S3 Vectors.

Contrôle d'accès dans Amazon S3

Dans AWS, une ressource est une entité avec laquelle vous pouvez travailler. Dans Amazon Simple Storage Service (S3), les compartiments et les objets sont les ressources Amazon S3 d'origine. Tous les clients de S3 possèdent généralement des compartiments contenant des objets. Au fur et à mesure que de nouvelles fonctionnalités ont été ajoutées à S3, des ressources supplémentaires ont également été ajoutées, mais tous les clients n'utilisent pas ces ressources spécifiques aux fonctionnalités. Pour plus d'informations sur les ressources Amazon S3, consultez Ressources S3.

Par défaut, toutes les ressources Amazon S3 sont privées. Par défaut également, l'utilisateur racine du Compte AWS qui a créé la ressource (propriétaire de la ressource) et les utilisateurs IAM de ce compte disposant des autorisations nécessaires peuvent accéder à une ressource qu'ils ont créée. Le propriétaire de la ressource décide qui d'autre peut y accéder, ainsi que les actions que ces tiers sont autorisés à effectuer au niveau de cette ressource. S3 propose divers outils de gestion des accès que vous pouvez utiliser pour accorder à des tiers l'accès à vos ressources S3.

Les sections suivantes présentent un aperçu des ressources S3, des outils de gestion des accès S3 disponibles et des cas d'utilisation les plus adaptés à chaque outil de gestion des accès. Les listes de ces sections visent à être exhaustives et incluent toutes les ressources S3, tous les outils de gestion des accès et tous les cas d'utilisation courants liés à la gestion des accès. Dans le même temps, ces sections sont conçues pour être des répertoires qui vous mèneront aux détails techniques que vous souhaitez. Si vous comprenez bien certaines des rubriques suivantes, vous pouvez passer directement à la section qui vous concerne.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Rubriques

- Ressources S3
- Identités
- Outils de gestion des accès
- Actions
- Cas d'utilisation de la gestion des accès
- Résolution des problèmes de gestion d'accès

Ressources S3

Les ressources Amazon S3 d'origine sont les compartiments et les objets qu'ils contiennent. Au fur et à mesure que de nouvelles fonctionnalités sont ajoutées à S3, de nouvelles ressources sont également ajoutées. La liste suivante est une liste complète des ressources S3 et de leurs fonctionnalités respectives.

Type de ressource	Fonctionnalité d'Amazon S3	Description
`bucket`	Fonctions de base	Un compartiment est un conteneur d'objets. Pour stocker un ou plusieurs objets dans S3, créez un compartiment, puis chargez-y les objets souhaités. Pour de plus amples informations, veuillez consulter Création, configuration et utilisation de compartiments à usage général Amazon S3.
`object`		Un objet peut être un fichier et toutes les métadonnées qui décrivent ce fichier. Lorsqu'un objet se trouve dans le compartiment, vous pouvez l'ouvrir, le télécharger et le déplacer. Pour de plus amples informations, veuillez consulter Utilisation des objets dans Amazon S3.
`accesspoint`	Points d'accès	Les points d'accès sont des points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations Amazon S3 sur des objets, notamment `GetObject` et `PutObject` . Chaque point d'accès applique des autorisations, des contrôles réseau et une stratégie de point d'accès personnalisée distincts, qui fonctionne conjointement avec la politique de compartiment associée au compartiment sous-jacent. Vous pouvez configurer n'importe quel point d'accès pour n'accepter que les demandes provenant d'un cloud privé virtuel (VPC) ou configurer des paramètres de blocage de l'accès public personnalisés pour chaque point d'accès. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Type de ressource	Fonctionnalité d'Amazon S3	Description
`objectlambdaaccesspoint`		Un point d'accès Object Lambda est un point d'accès de compartiment qui est également associé à une fonction Lambda. Avec un point d'accès Object Lambda, vous pouvez ajouter votre propre code aux demandes Amazon S3 `GET`, `LIST` et `HEAD` afin de modifier et de traiter les données lorsqu'elles sont renvoyées vers une application. Pour de plus amples informations, veuillez consulter Création de points d'accès Object Lambda.
`multiregionaccesspoint`		Les points d'accès multi-régions fournissent un point de terminaison global que les applications peuvent utiliser pour traiter les demandes provenant de compartiments Amazon S3 situés dans plusieurs régions AWS . Vous pouvez utiliser des points d'accès multi-régions pour créer des applications multi-régions avec la même architecture utilisée dans une seule région, puis exécuter ces applications partout dans le monde. Au lieu d'envoyer des demandes via l'Internet public congestionné, les demandes d'application adressées à un point d'accès global multirégional sont automatiquement acheminées via le réseau AWS mondial vers le compartiment Amazon S3 le plus proche. Pour de plus amples informations, veuillez consulter Gestion du trafic multirégional avec des points d'accès multirégionaux.
`job`	Opérations par lot S3	Une tâche est une ressource de la fonctionnalité d'opérations par lot S3. Vous pouvez utiliser les opérations par lot S3 pour effectuer des opérations par lot à grande échelle sur des objets Amazon S3 que vous spécifiez. Amazon S3 suit la progression de la tâche d'opérations par lot, envoie des notifications et stocke un rapport de fin de tâche détaillé sur toutes les actions, offrant ainsi une expérience sans serveur entièrement gérée et qui peut être vérifiée. Pour de plus amples informations, veuillez consulter Exécution d'opérations groupées sur des objets avec les opérations par lot.

Type de ressource	Fonctionnalité d'Amazon S3	Description
`storagelensconfiguration`	S3 Storage Lens	Une configuration S3 Storage Lens collecte des métriques de stockage et des données utilisateur à l'échelle de l'organisation entre les différents comptes. S3 Storage Lens fournit aux administrateurs une vue unique de l'utilisation et de l'activité du stockage des objets sur des centaines, voire des milliers, de comptes au sein d'une organisation, avec des détails permettant de générer des informations exploitables à plusieurs niveaux d'agrégation. Pour de plus amples informations, veuillez consulter Évaluer l'activité et l'utilisation de votre stockage avec Amazon S3 Storage Lens.
`storagelensgroup`		Un groupe S3 Storage Lens regroupe les métriques à l'aide de filtres personnalisés basés sur les métadonnées des objets. Les groupes S3 Storage Lens vous permettent d'analyser les caractéristiques de vos données, telles que la répartition des objets par ancienneté, les types de fichiers les plus courants, etc. Pour de plus amples informations, veuillez consulter Utilisation des groupes S3 Storage Lens pour filtrer et agréger des métriques.
`accessgrantsinstance`	Autorisations d'accès S3	Une instance d'autorisations d'accès S3 est un conteneur pour les autorisations S3 que vous créez. Avec les d'autorisations d'accès S3, vous pouvez créer des autorisations pour vos données Amazon S3 pour les identités IAM au sein de votre compte, les identités IAM dans d'autres comptes (autorisations intercomptes) et les identités d'annuaire e ajoutées à AWS IAM Identity Center à partir de votre annuaire d'entreprise. Pour plus d'informations sur les autorisations d'accès S3, consultez Gestion de l'accès avec les autorisations d'accès S3.

Type de ressource	Fonctionnalité d'Amazon S3	Description
`accessgrantslocation`		Un emplacement d'autorisations d'accès est un compartiment, un préfixe dans un compartiment ou un objet que vous enregistrez dans votre instance d'autorisations d'accès S3. Vous devez enregistrer des emplacements au sein de l'instance d'autorisations d'accès S3 avant de pouvoir créer une autorisation pour cet emplacement. Ensuite, avec S3 Access Grants, vous pouvez accorder l'accès au compartiment, au préfixe ou à l'objet pour les identités IAM de votre compte, les identités IAM d'autres comptes (comptes multiples) et les identités de répertoire ajoutées à AWS IAM Identity Center partir de votre annuaire d'entreprise. Pour plus d'informations sur les autorisations d'accès S3, consultez Gestion de l'accès avec les autorisations d'accès S3.
`accessgrant`		Une autorisation d'accès est une autorisation individuelle accordée à vos données Amazon S3. Avec S3 Access Grants, vous pouvez créer des autorisations pour vos données Amazon S3 pour les identités IAM au sein de votre compte, les identités IAM sur d'autres comptes (comptes intercomptes) et les identités de répertoire ajoutées à AWS IAM Identity Center partir de votre annuaire d'entreprise. Pour plus d'informations sur les autorisations d'accès S3, consultez Gestion de l'accès avec les autorisations d'accès S3.

Compartiments

Il existe deux types de compartiments Amazon S3 : les compartiments à usage général et les compartiments de répertoires.

- Les compartiments à usage général constituent le type de compartiment S3 d'origine et sont recommandés pour la plupart des cas d'utilisation et des modèles d'accès. Les compartiments à usage général autorisent également les objets stockés dans toutes les classes de stockage, à

l'exception de S3 Express One Zone. Pour plus d'informations sur les classes de stockage S3, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

- Les compartiments de répertoires utilisent la classe de stockage S3 Express One Zone, recommandée si votre application est sensible aux performances et peut bénéficier d'une latence inférieure à dix millisecondes pour les demandes PUT et GET. Pour plus d'informations, consultez Utilisation des compartiments de répertoires, S3 Express One Zone et Autorisation des opérations d'API de point de terminaison régional avec IAM.

Catégorisation des ressources S3

Amazon S3 fournit des fonctionnalités permettant de catégoriser et d'organiser vos ressources S3. La catégorisation de vos ressources est non seulement utile pour les organiser, mais vous pouvez également définir des règles de gestion des accès en fonction des catégories de ressources. Plus spécifiquement, les préfixes et le balisage sont deux fonctionnalités d'organisation du stockage que vous pouvez utiliser lors de la définition des autorisations de gestion des accès.

> **Note**
>
> Les informations suivantes s'appliquent aux compartiments à usage général. Les compartiments de répertoires ne prennent pas en charge le balisage, et leurs préfixes sont soumis à certains limites. Pour de plus amples informations, veuillez consulter Autorisation des opérations d'API de point de terminaison régional avec IAM.

- Préfixe : un préfixe est une chaîne de caractères située au début d'un nom de clé d'objet et qui sert à organiser les objets stockés dans vos compartiments S3. Vous pouvez utiliser un caractère séparateur, tel qu'une barre oblique (/), pour indiquer la fin du préfixe dans le nom de la clé de l'objet. Par exemple, vous pouvez avoir des noms de clé d'objet qui commencent par le préfixe `engineering/` ou `marketing/campaigns/`. L'utilisation d'un délimiteur à la fin du préfixe, tel qu'une barre oblique, `/`, émule les conventions de dénomination des dossiers et des fichiers. Toutefois, dans S3, le préfixe fait partie du nom de la clé d'objet. Dans les compartiments S3 à usage général, il n'existe pas de hiérarchie de dossiers réelle.

  Amazon S3 permet d'organiser et de regrouper les objets à l'aide de leur préfixe. Vous pouvez également gérer l'accès aux objets à l'aide de leur préfixe. Par exemple, vous pouvez limiter l'accès aux seuls objets dont le nom commence par un préfixe spécifique.

Pour de plus amples informations, veuillez consulter Organisation des objets à l'aide de préfixes. La console S3 utilise le concept de dossiers, qui, dans les compartiments à usage général, sont essentiellement des préfixes ajoutés au nom de la clé de l'objet. Pour de plus amples informations, veuillez consulter Organisation des objets dans la console Amazon S3 à l'aide de dossiers.

- Balise : une balise est une paire clé-valeur que vous allouez aux ressources. Par exemple, vous pouvez baliser certaines ressources avec la balise `topicCategory=engineering`. Vous pouvez utiliser le balisage pour faciliter la répartition des coûts, la catégorisation et l'organisation, ainsi que le contrôle d'accès. Le balisage des compartiments est uniquement utilisé pour la répartition des coûts. Vous pouvez baliser des objets, S3 Storage Lens, des tâches et des autorisations d'accès S3 à des fins d'organisation ou de contrôle d'accès. Dans les autorisations d'accès S3, vous pouvez également utiliser le balisage pour la répartition des coûts. À titre d'exemple de contrôle de l'accès aux ressources à l'aide de leurs balises, vous pouvez ne partager que les objets dotés d'une balise spécifique ou d'une combinaison de balises.

  Pour plus d'informations, consultez Contrôle de l'accès aux ressources AWS à l'aide de balises de ressources dans le Guide de l'utilisateur IAM.

Identités

Dans Amazon S3, le propriétaire de la ressource est l'identité qui a créé la ressource, telle qu'un compartiment ou un objet. Par défaut, seul l'utilisateur racine du compte qui a créé la ressource et les identités IAM du compte disposant de l'autorisation requise peuvent accéder à la ressource S3. Les propriétaires de ressources peuvent autoriser d'autres identités à accéder à leurs ressources S3.

Les identités qui ne possèdent pas une ressource peuvent demander l'accès à cette ressource. Les demandes adressées à une ressource sont soit authentifiées, soit non authentifiées. Les demandes authentifiées doivent inclure une valeur de signature qui authentifie l'expéditeur de la demande. Les demandes non authentifiées ne nécessitent pas de signature. Nous vous recommandons de n'accorder l'accès qu'aux utilisateurs authentifiés. Pour plus d'informations sur l'authentification des demandes, consultez Demandes dans la Référence d'API Amazon S3.

> **Important**
>
> Nous vous recommandons de ne pas utiliser les informations d'identification de l'utilisateur Compte AWS root pour effectuer des demandes authentifiées. Il est préférable de créer un rôle IAM, puis de lui accorder un accès total. Nous appelons les utilisateurs possédant ce rôle des administrateurs. Vous pouvez utiliser les informations d'identification attribuées au

rôle d'administrateur, au lieu des informations d'identification de l'utilisateur Compte AWS root, pour interagir avec AWS et effectuer des tâches, telles que créer un bucket, créer des utilisateurs et accorder des autorisations. Pour plus d'informations, consultez Informations d'identification d'utilisateur racine de Compte AWS et informations d'identification d'utilisateur IAM dans Références générales AWS. Consultez aussi Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Les identités qui accèdent à vos données dans Amazon S3 peuvent être les suivantes :

Compte AWS owner

Celui Compte AWS qui a créé la ressource. Par exemple, le compte qui a créé le compartiment. Ce compte possède la ressource. Pour plus d'informations, consultez Utilisateur racine AWS.

Identités IAM dans le même compte que le propriétaire Compte AWS

Lors de la configuration de comptes pour les nouveaux membres de l'équipe qui ont besoin d'un accès S3, le Compte AWS propriétaire peut utiliser AWS Identity and Access Management (IAM) pour créer des utilisateurs, des groupes et des rôles. Le Compte AWS propriétaire peut ensuite partager des ressources avec ces identités IAM. Le propriétaire du compte peut également spécifier les autorisations à attribuer aux identités IAM, qui autorisent ou refusent les actions pouvant être effectuées sur les ressources partagées.

Les identités IAM offrent des fonctionnalités accrues, notamment la possibilité d'exiger des utilisateurs qu'ils saisissent des informations d'identification de connexion avant d'accéder aux ressources partagées. Avec les identités IAM, vous pouvez mettre en œuvre une forme d'authentification multifactorielle (MFA) IAM pour prendre en charge une base d'identité solide. L'une des bonnes pratiques IAM consiste à créer des rôles pour la gestion des accès au lieu d'accorder des autorisations à chaque utilisateur individuel. Vous attribuez le rôle approprié à chaque utilisateur. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM.

Autres titulaires de AWS comptes et leurs identités IAM (accès entre comptes)

Le Compte AWS propriétaire peut également donner accès aux ressources à d'autres propriétaires de AWS comptes, ou à des identités IAM appartenant à un autre AWS compte.

> **Note**
>
> Délégation d'autorisations : si un Compte AWS possède une ressource, il peut accorder ces autorisations à un autre Compte AWS. Ce compte peut alors déléguer aux utilisateurs du même compte l'ensemble de ces autorisations ou un sous-ensemble de celles-ci. Cela s'appelle une délégation d'autorisations. Cependant, un compte qui reçoit des autorisations d'un autre compte ne peut pas déléguer ces autorisations « intercomptes » à un autre Compte AWS.

Utilisateurs anonymes (accès public)

Le Compte AWS propriétaire peut rendre les ressources publiques. D'un point de vue technique, rendre une ressource publique consiste à partager la ressource avec l'utilisateur anonyme. Les compartiments créés depuis avril 2023 bloquent tout accès public par défaut, sauf si vous modifiez ce paramètre. Nous vous recommandons de configurer vos compartiments de sorte qu'ils bloquent l'accès public, et de n'accorder l'accès qu'aux utilisateurs authentifiés. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

Services AWS

Le propriétaire de la ressource peut accorder à un autre AWS service l'accès à une ressource Amazon S3. Par exemple, vous pouvez accorder au AWS CloudTrail service l'`s3:PutObject`autorisation d'écrire des fichiers journaux dans votre compartiment. Pour plus d'informations, consultez la section Fournir l'accès à un AWS service.

Identités des annuaires d'entreprise

Le propriétaire de la ressource peut accorder à des utilisateurs ou à des rôles de votre annuaire d'entreprise l'accès à une ressource S3 à l'aide des autorisations d'accès S3. Pour plus d'informations sur l'ajout de votre annuaire d'entreprise à AWS IAM Identity Center, voir Qu'est-ce qu'IAM Identity Center ? .

Propriétaires du compartiment ou de la ressource

Celui Compte AWS que vous utilisez pour créer des buckets et télécharger des objets possède ces ressources. Un propriétaire de compartiment peut accorder à un autre Compte AWS (ou à des utilisateurs d'un autre compte) des autorisations intercomptes pour charger des objets.

Lorsqu'un propriétaire de compartiment autorise un autre compte à charger des objets dans un compartiment, le propriétaire du compartiment est propriétaire par défaut de tous les objets chargés dans son compartiment. Toutefois, si les paramètres de bucket appliqués par le propriétaire du bucket et les paramètres de bucket préférés du propriétaire du bucket sont désactivés, le Compte AWS responsable du téléchargement des objets est propriétaire de ces objets, et le propriétaire du bucket n'a aucune autorisation sur les objets appartenant à un autre compte, avec les exceptions suivantes :

- Le propriétaire du compartiment paie les factures. Le propriétaire du compartiment peut refuser l'accès aux objets ou supprimer des objets dans le compartiment, quel que soit le propriétaire de ces derniers.
- Le propriétaire du compartiment peut archiver n'importe quel objet ou restaurer des objets archivés, quel qu'en soit le propriétaire. L'archivage fait référence à la classe de stockage utilisée pour stocker les objets. Pour de plus amples informations, veuillez consulter Gestion du cycle de vie des objets.

Outils de gestion des accès

Amazon S3 fournit plusieurs fonctionnalités et outils de sécurité. Vous trouverez ci-dessous une liste complète de ces fonctionnalités et outils. Vous n'avez pas besoin de tous ces outils de gestion des accès, mais vous devez en utiliser un ou plusieurs pour accorder l'accès à vos ressources Amazon S3. Une utilisation adéquate de ces outils contribue à garantir que vos ressources ne sont accessibles qu'aux utilisateurs prévus.

L'outil de gestion des accès le plus couramment utilisé est une stratégie d'accès. Une politique d'accès peut être une politique basée sur les ressources attachée à une AWS ressource, telle qu'une politique de compartiment pour un compartiment. Une stratégie d'accès peut également être une politique basée sur l'identité. Dans ce cas, elle est associée à une identité AWS Identity and Access Management (IAM), telle qu'un utilisateur, un groupe ou un rôle IAM. Rédigez une politique d'accès pour accorder Comptes AWS aux utilisateurs, aux groupes et aux rôles IAM l'autorisation d'effectuer des opérations sur une ressource. Par exemple, vous pouvez accorder une `PUT Object` autorisation à un autre compte Compte AWS afin qu'il puisse télécharger des objets dans votre compartiment.

Une stratégie d'accès décrit qui a accès à quoi. Lorsqu'Amazon S3 reçoit une demande, toutes les stratégies d'accès doivent être évaluées afin de déterminer si cette demande doit être autorisée ou refusée. Pour plus d'informations sur la manière dont Amazon S3 évalue ces politiques, consultez Comment Amazon S3 autorise une demande.

Les outils de gestion de l'accès disponibles dans Amazon S3 sont les suivants.

Politique de compartiment

Une politique de compartiment Amazon S3 est une politique AWS Identity and Access Management (IAM) basée sur les ressources, au format JSON. Elle est associée à un compartiment particulier. Utilisez des politiques de compartiment pour accorder des autorisations à d'autres identités Comptes AWS ou à des identités IAM pour le compartiment et les objets qu'il contient. De nombreux cas d'utilisation de la gestion des accès S3 peuvent être satisfaits au moyen d'une politique de compartiment. Avec les politiques de compartiment, vous pouvez personnaliser l'accès au compartiment pour vous assurer que seules les identités que vous avez approuvées peuvent accéder aux ressources et effectuer des actions en leur sein. Pour de plus amples informations, veuillez consulter Politiques de compartiment pour Amazon S3.

Voici un exemple de politique de compartiment. Vous exprimez la politique de compartiment à l'aide d'un fichier JSON. Cet exemple de politique accorde à un rôle IAM l'autorisation de lecture sur tous les objets du compartiment. Il contient une instruction appelée `BucketLevelReadPermissions`, qui autorise l'action `s3:GetObject` (autorisation de lecture) sur les objets contenus dans un compartiment appelé `amzn-s3-demo-bucket1`. En spécifiant un rôle IAM comme `Principal`, cette politique accorde l'accès à tout utilisateur IAM qui endosse ce rôle. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid":"BucketLevelReadPermissions",
      "Effect":"Allow",
      "Principal": {
     "AWS": "arn:aws:iam::123456789101:role/s3-role"
      },
      "Action":["s3:GetObject"],
      "Resource":["arn:aws:s3:::amzn-s3-demo-bucket/*"]
    }]
  }
```

> **Note**
>
> Lors de la création de politiques, évitez d'utiliser des caractères génériques (*) dans l'élément `Principal`, car cela permet à quiconque d'accéder effectivement à vos ressources Amazon S3. Au lieu de cela, répertoriez explicitement les utilisateurs ou les groupes autorisés à accéder au compartiment ou répertoriez les conditions qui doivent être remplies à l'aide d'une clause de condition dans la stratégie. Au lieu d'inclure un caractère générique pour les actions de vos utilisateurs ou de vos groupes, accordez-leur des autorisations spécifiques le cas échéant.

Politique basée sur l'identité

Une politique utilisateur IAM ou basée sur l'identité est un type de politique AWS Identity and Access Management (IAM). Une politique basée sur l'identité est une politique au format JSON associée aux utilisateurs, groupes ou rôles IAM dans votre compte AWS . Vous pouvez utiliser des politiques basées sur l'identité pour accorder à une identité IAM l'accès à vos compartiments ou objets. Vous pouvez créer des utilisateurs, des groupes et des rôles IAM dans votre compte et leur attacher des stratégies d'accès. Vous pouvez ensuite accorder l'accès aux ressources AWS , notamment aux ressources Amazon S3. Pour de plus amples informations, veuillez consulter Politiques basées sur l'identité pour Amazon S3.

Un exemple de politique basée sur l'identité est présenté ci-dessous. Cet exemple de politique permet au rôle IAM qui y est associé d'exécuter six actions Amazon S3 différentes (autorisations) sur un compartiment et sur les objets qu'il contient. Si vous associez cette politique à un rôle IAM dans votre compte et que vous attribuez ce rôle à certains de vos utilisateurs IAM, les utilisateurs dotés de ce rôle pourront effectuer ces actions sur les ressources (compartiments) spécifiées dans votre politique. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Sid": "AssignARoleActions",
    "Effect": "Allow",
```

```
    "Action": [
   "s3:PutObject",
   "s3:GetObject",
   "s3:ListBucket",
   "s3:DeleteObject",
   "s3:GetBucketLocation"
    ],
    "Resource": [
   "arn:aws:s3:::amzn-s3-demo-bucket/*",
   "arn:aws:s3:::amzn-s3-demo-bucket"
    ]
    },
  {
    "Sid": "AssignARoleActions2",
    "Effect": "Allow",
    "Action": "s3:ListAllMyBuckets",
    "Resource": "*"
  }
  ]
}
```

Autorisations d'accès S3

Utilisez les autorisations d'accès S3 pour créer des autorisations d'accès à vos données Amazon S3 pour les identités figurant dans les annuaires d'identités d'entreprise, telles qu'Active Directory, et les identités AWS Identity and Access Management (IAM). Les autorisations d'accès S3 vous aident à gérer les autorisations de données à l'échelle. En outre, les autorisations d'accès S3 enregistrent l'identité de l'utilisateur final et l'application utilisée pour accéder aux données S3 dans AWS CloudTrail. Cela fournit un historique d'audit détaillé remontant jusqu'à l'identité de l'utilisateur final pour tous les accès aux données de vos compartiments S3. Pour de plus amples informations, veuillez consulter Gestion de l'accès avec les autorisations d'accès S3.

Points d'accès

Les points d'accès Amazon S3 simplifient la gestion de l'accès aux données à l'échelle pour les applications utilisant des jeux de données partagés dans S3. Les points d'accès sont appelés points de terminaison réseau. Ils sont associés à un compartiment. Vous pouvez utiliser des points d'accès pour effectuer des opérations sur des objets S3 à l'échelle, comme le chargement et l'extraction d'objets. Jusqu'à 10 000 points d'accès peuvent être associés à un compartiment. Et pour chaque point d'accès, vous pouvez appliquer des autorisations et des contrôles réseau distincts pour vous

donner un contrôle précis sur l'accès à vos objets S3. Les points d'accès S3 peuvent être associés à des compartiments du même compte ou d'un autre compte approuvé. Les stratégies de points d'accès sont basées sur les ressources. Elles sont évaluées conjointement avec la politique de compartiment sous-jacente. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Liste de contrôle d'accès (ACL)

Une ACL est une liste de subventions identifiant le bénéficiaire et l'autorisation accordée. ACLs accorder des autorisations de lecture ou d'écriture de base à d'autres Comptes AWS. ACLs utilisez un schéma XML spécifique à Amazon S3. Une liste ACL est un type de politique AWS Identity and Access Management (IAM). Une liste ACL d'objet est utilisée pour gérer l'accès à un objet, tandis qu'une liste ACL de compartiment est utilisée pour gérer l'accès à un compartiment. Avec les politiques de compartiment, il existe une seule politique pour l'ensemble du compartiment, mais ACLs les objets sont spécifiés pour chaque objet. Nous vous recommandons de rester ACLs éteint, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès individuellement pour chaque objet. Pour plus d'informations sur l'utilisation ACLs, consultezContrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

> **Warning**
>
> La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent pas l'utilisation de ACLs.

Voici un exemple de liste ACL de compartiment. L'autorisation dans la liste ACL montre que le propriétaire du compartiment dispose d'une autorisation de contrôle total.

```
<?xml version="1.0" encoding="UTF-8"?>
 <AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
   <ID>Owner-Canonical-User-ID</ID>
   <DisplayName>owner-display-name</DisplayName>
  </Owner>
 <AccessControlList>
  <Grant>
   <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Canonical
 User">
    <ID>Owner-Canonical-User-ID</ID>
```

```
    <DisplayName>display-name</DisplayName>
   </Grantee>
   <Permission>FULL_CONTROL</Permission>
  </Grant>
 </AccessControlList>
</AccessControlPolicy>
```

Propriétaire de l'objet

Pour gérer l'accès à vos objets, vous devez en être le propriétaire. Utilisez le paramètre Propriétaire de l'objet au niveau du compartiment pour contrôler la propriété des objets chargés dans votre compartiment. Utilisez également la propriété des objets pour l'activer ACLs. Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket et tous les paramètres ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère exclusivement l'accès aux données. Pour gérer l'accès, le propriétaire du compartiment utilise des politiques ou un autre outil de gestion des accès, à l'exception de ACLs. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

La propriété des objets comporte trois paramètres que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre bucket et pour les activer ACLs :

ACLs éteint

- Appliqués par le propriétaire du compartiment (par défaut) : ACLs sont désactivés, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. ACLs n'affectent pas les autorisations relatives aux données du compartiment S3. Le compartiment utilise des stratégies exclusivement pour définir le contrôle des accès.

ACLs activé

- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.
- Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

Bonnes pratiques supplémentaires

Envisagez d'utiliser les outils de compartiment suivants pour protéger les données en transit et au repos, qui sont toutes essentielles pour préserver l'intégrité et l'accessibilité de vos données.

- Bloquer l'accès public : ne désactivez pas le paramètre par défaut Bloquer l'accès public au niveau du compartiment. Ce paramètre bloque par défaut l'accès public à vos données. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.
- Gestion des versions S3 : pour garantir l'intégrité des données, vous pouvez implémenter le paramètre de gestion des versions du compartiment S3, qui attribue des versions à vos objets au fur et à mesure des mises à jour, au lieu de les remplacer. Vous pouvez utiliser la gestion des versions S3 pour préserver, récupérer et restaurer une version précédente, si nécessaire. Pour en savoir plus sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.
- Verrouillage d'objet S3 : le verrouillage d'objet S3 est un autre paramètre que vous pouvez implémenter pour assurer l'intégrité des données. Cette fonctionnalité peut implémenter un modèle write-once-read-many (WORM) pour stocker des objets de manière immuable. Pour en savoir plus sur le verrouillage d'objet, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.
- Chiffrement des objets : Amazon S3 offre plusieurs options de chiffrement d'objet qui protègent les données en transit et au repos. Le chiffrement côté serveur chiffre vos objets avant de les enregistrer sur les disques des centres de données, puis les déchiffre lorsque vous téléchargez les objets. Si vous authentifiez votre demande et que vous avez les autorisations d'accès requises, il n'y a aucune différence dans la manière dont vous accédez aux objets chiffrés ou déchiffrés. Pour de plus amples informations, veuillez consulter Protection des données avec le chiffrement côté serveur. S3 chiffre les objets récemment chargés par défaut. Pour de plus amples informations, veuillez consulter Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Le chiffrement côté client consiste à chiffrer des données avant de les envoyer à Amazon S3. Pour de plus amples informations, veuillez consulter Protection des données avec le chiffrement côté client.
- Méthodes de signature — Signature Version 4 est le processus d'ajout d'informations d'authentification aux AWS demandes envoyées par HTTP. Pour des raisons de sécurité, la plupart des demandes AWS doivent être signées avec une clé d'accès, qui consiste en un identifiant de clé d'accès et une clé d'accès secrète. Ces deux clés sont généralement appelées informations d'identification de sécurité. Pour plus d'informations, consultez les sections Authentification des demandes (AWS Signature version 4) et Processus de signature Signature version 4.

Actions

Pour obtenir la liste complète des autorisations et des clés de condition S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Actions

Les actions AWS Identity and Access Management (IAM) pour Amazon S3 sont les actions possibles qui peuvent être effectuées sur un compartiment ou un objet S3. Vous accordez ces actions aux identités afin qu'elles puissent agir sur vos ressources S3. Parmi les exemples d'actions S3, citons `s3:GetObject` qui permet de lire des objets dans un compartiment et `s3:PutObject` qui permet d'écrire des objets dans un compartiment.

Clés de condition

Outre les actions, les clés de condition IAM n'accordent l'accès que lorsqu'une condition est remplie. Les clés de condition sont facultatives.

> **Note**
>
> Dans une stratégie d'accès basée sur les ressources, telle qu'une politique de compartiment, ou dans une politique basée sur l'identité, vous pouvez spécifier les éléments suivants :
>
> - Une action ou un ensemble d'actions figurant dans l'élément `Action` de la déclaration de politique.
> - Dans l'élément `Effect`de la déclaration de politique, vous pouvez spécifier `Allow` pour autoriser les actions répertoriées, ou `Deny` pour bloquer les actions indiquées. Pour assurer la pratique du moindre privilège, les instructions `Deny` dans l'élément `Effect` de la stratégie d'accès doivent être aussi larges que possible alors que les instructions `Allow` doivent être aussi restreintes que possible. Les effets des instructions `Deny` associés à l'action `s3:*` sont un autre bon moyen de mettre en œuvre des bonnes pratiques d'activation pour les identités incluses dans des déclarations de condition de politique.
> - Une clé de condition dans l'élément `Condition` d'une déclaration de politique.

Cas d'utilisation de la gestion des accès

Amazon S3 fournit aux propriétaires de ressources une variété d'outils pour accorder l'accès. L'outil de gestion des accès S3 que vous utilisez dépend des ressources S3 que vous souhaitez partager, des identités auxquelles vous accordez l'accès et des actions que vous souhaitez autoriser ou refuser. Vous pouvez utiliser un ou plusieurs outils de gestion d'accès S3 pour gérer l'accès à vos ressources S3.

Dans la plupart des cas, vous pouvez utiliser une stratégie d'accès pour gérer les autorisations. Une politique d'accès peut être une politique basée sur les ressources, qui est attachée à une ressource telle qu'un compartiment ou à une autre ressource Amazon S3 (Ressources S3). Une politique d'accès peut également être une politique basée sur l'identité, attachée à un utilisateur, un groupe ou un rôle AWS Identity and Access Management (IAM) dans votre compte. Vous constaterez peut-être qu'une politique de compartiment convient mieux à votre cas d'utilisation. Pour de plus amples informations, veuillez consulter Politiques de compartiment pour Amazon S3. Par ailleurs, avec AWS Identity and Access Management (IAM), vous pouvez créer des utilisateurs, des groupes et des rôles IAM au sein de votre entreprise et gérer leur accès aux compartiments Compte AWS et aux objets par le biais de politiques basées sur l'identité. Pour de plus amples informations, veuillez consulter Politiques basées sur l'identité pour Amazon S3.

Pour vous aider à utiliser ces options de gestion des accès, vous trouverez ci-dessous des cas d'utilisation courants de clients Amazon S3 et des recommandations pour chacun des outils de gestion des accès S3.

Le Compte AWS propriétaire souhaite partager des buckets uniquement avec les utilisateurs du même compte

Tous les outils de gestion des accès peuvent répondre à ce cas d'utilisation de base. Nous recommandons les outils suivants de gestion des accès pour ce cas d'utilisation :

- Politique de compartiment : si vous souhaitez accorder l'accès à un compartiment ou à un petit nombre de compartiments, ou si vos autorisations d'accès aux compartiments sont similaires d'un compartiment à l'autre, utilisez une politique de compartiment. Avec les politiques de compartiment, vous gérez une seule politique pour chaque compartiment. Pour de plus amples informations, veuillez consulter Politiques de compartiment pour Amazon S3.
- Politique basée sur l'identité : si vous avez un très grand nombre de compartiments dotés d'autorisations d'accès différentes pour chaque compartiment et que vous ne devez gérer que quelques rôles utilisateur, vous pouvez utiliser une politique IAM pour les utilisateurs, les groupes

ou les rôles. Les politiques IAM sont également une bonne option si vous gérez l'accès des utilisateurs à d'autres AWS ressources, ainsi qu'aux ressources Amazon S3. Pour de plus amples informations, veuillez consulter Exemple 1 : propriétaire d'un compartiment accordant à ses utilisateurs des autorisations sur un compartiment.

- Autorisations d'accès S3 : vous pouvez utiliser les autorisations d'accès S3 pour accorder l'accès à vos compartiments, préfixes ou objets S3. Les autorisations d'accès S3 vous permettent de spécifier différentes autorisations au niveau des objets à l'échelle, tandis que les politiques de compartiment sont limitées à une taille de 20 Ko. Pour de plus amples informations, veuillez consulter Bien démarrer avec les autorisations d'accès S3.
- Points d'accès : vous pouvez utiliser des points d'accès, qui sont des points de terminaison réseau associés à un compartiment. Jusqu'à 10 000 points d'accès peuvent être associés à un compartiment. Et pour chaque point d'accès, vous pouvez appliquer des autorisations et des contrôles réseau distincts pour vous donner un contrôle précis sur l'accès à vos objets S3. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Le Compte AWS propriétaire souhaite partager des buckets ou des objets avec des utilisateurs d'un autre AWS compte (comptes croisés)

Pour accorder une autorisation à une autre personne Compte AWS, vous devez utiliser une politique de compartiment ou l'un des outils de gestion des accès recommandés ci-dessous. Vous ne pouvez pas utiliser de stratégie d'accès basée sur l'identité pour ce cas d'utilisation. Pour plus d'informations sur l'octroi d'un accès intercompte, consultez Comment puis-je fournir un accès intercompte aux objets stockés dans des compartiments Simple Storage Service (Amazon S3) ?.

Nous recommandons les outils suivants de gestion des accès pour ce cas d'utilisation :

- Politique de compartiment : avec les politiques de compartiment, vous gérez une politique pour chaque compartiment. Pour de plus amples informations, veuillez consulter Politiques de compartiment pour Amazon S3.
- Autorisations d'accès S3 : vous pouvez utiliser les autorisations d'accès S3 pour accorder des autorisations intercomptes à vos compartiments, préfixes ou objets S3. Vous pouvez utiliser les autorisations d'accès S3 pour spécifier différentes autorisations au niveau des objets à l'échelle, tandis que les politiques de compartiment sont limitées à une taille de 20 Ko. Pour de plus amples informations, veuillez consulter Bien démarrer avec les autorisations d'accès S3.

- Points d'accès : vous pouvez utiliser des points d'accès, qui sont des points de terminaison réseau associés à un compartiment. Jusqu'à 10 000 points d'accès peuvent être associés à un compartiment. Et pour chaque point d'accès, vous pouvez appliquer des autorisations et des contrôles réseau distincts pour vous donner un contrôle précis sur l'accès à vos objets S3. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Le Compte AWS propriétaire ou le propriétaire du compartiment doit accorder des autorisations au niveau de l'objet ou du préfixe, et ces autorisations varient d'un objet à l'autre ou d'un préfixe à l'autre

Dans une politique de compartiment, par exemple, vous pouvez accorder l'accès aux objets d'un compartiment qui partagent un préfixe de nom de clé spécifique ou qui possèdent une balise spécifique. Vous pouvez octroyer des autorisations en lecture sur les objets portant le préfixe de nom de clé `logs/`. Néanmoins, si vos autorisations d'accès varient par objet, l'octroi d'autorisations à des objets individuels à l'aide d'une politique de compartiment peut s'avérer peu pratique, d'autant plus que les politiques de compartiment sont limitées à une taille de 20 Ko.

Nous recommandons les outils suivants de gestion des accès pour ce cas d'utilisation :

- Autorisations d'accès S3 : vous pouvez utiliser les autorisations d'accès S3 pour gérer les autorisations au niveau de l'objet ou du préfixe. Contrairement aux politiques de compartiment, les autorisations d'accès S3 vous permettent de spécifier différentes autorisations au niveau des objets à l'échelle. Les politiques de compartiment sont limitées à une taille de 20 Ko. Pour de plus amples informations, veuillez consulter Bien démarrer avec les autorisations d'accès S3.
- Points d'accès : vous pouvez utiliser des points d'accès pour gérer les autorisations au niveau des objets ou des préfixes. Les points d'accès sont appelés points de terminaison réseau. Ils sont associés à un compartiment. Jusqu'à 10 000 points d'accès peuvent être associés à un compartiment. Et pour chaque point d'accès, vous pouvez appliquer des autorisations et des contrôles réseau distincts pour vous donner un contrôle précis sur l'accès à vos objets S3. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .
- ACLs— Nous vous déconseillons d'utiliser les listes de contrôle d'accès (ACLs), notamment parce qu' ACLs elles sont limitées à 100 autorisations par objet. Toutefois, si vous choisissez de l'activer ACLs, dans les paramètres de votre bucket, définissez Object Ownership sur Bucket owner preferred and ACLsenabled. Avec ce paramètre, de nouveaux objets écrits avec la liste ACL

`bucket-owner-full-control` prédéfinie sont automatiquement détenus par le propriétaire du compartiment plutôt que par l'auteur d'objets. Vous pouvez ensuite utiliser un objet ACLs, qui est une politique d'accès au format XML, pour autoriser d'autres utilisateurs à accéder à l'objet. Pour de plus amples informations, veuillez consulter Présentation de la liste de contrôle d'accès (ACL).

Le Compte AWS propriétaire ou le propriétaire du bucket souhaite limiter l'accès au bucket uniquement à un compte spécifique IDs

Nous recommandons les outils suivants de gestion des accès pour ce cas d'utilisation :

- Politique de compartiment : avec les politiques de compartiment, vous gérez une politique pour chaque compartiment. Pour de plus amples informations, veuillez consulter Politiques de compartiment pour Amazon S3.
- Points d'accès : les points d'accès sont appelés points de terminaison réseau. Ils sont associés à un compartiment. Jusqu'à 10 000 points d'accès peuvent être associés à un compartiment. Et pour chaque point d'accès, vous pouvez appliquer des autorisations et des contrôles réseau distincts pour vous donner un contrôle précis sur l'accès à vos objets S3. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Le Compte AWS propriétaire ou le propriétaire du bucket souhaite disposer de points de terminaison distincts pour chaque utilisateur ou application qui accède à ses données

Nous recommandons l'outil suivant de gestion des accès pour ce cas d'utilisation :

- Points d'accès : les points d'accès sont appelés points de terminaison réseau. Ils sont associés à un compartiment. Jusqu'à 10 000 points d'accès peuvent être associés à un compartiment. Et pour chaque point d'accès, vous pouvez appliquer des autorisations et des contrôles réseau distincts pour vous donner un contrôle précis sur l'accès à vos objets S3. Chaque point d'accès applique une stratégie de point d'accès personnalisée qui fonctionne conjointement avec la politique de compartiment associée au compartiment sous-jacent. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Le Compte AWS propriétaire ou le propriétaire du bucket doit gérer l'accès depuis les points de terminaison Virtual Private Cloud (VPC) pour S3

Les points de terminaison de cloud privé virtuel (VPC) pour Amazon S3 sont des entités logiques au sein d'un VPC. qui autorisent la connectivité uniquement à S3. Nous recommandons les outils suivants de gestion des accès pour ce cas d'utilisation :

- Compartiments dans un VPC : vous pouvez utiliser une politique de compartiment pour contrôler qui est autorisé à accéder à vos compartiments et à quels points de terminaison de VPC ils peuvent accéder. Pour de plus amples informations, veuillez consulter Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment.
- Points d'accès : si vous choisissez de configurer des points d'accès, vous pouvez utiliser une politique de point d'accès. Vous pouvez configurer n'importe quel point d'accès pour accepter uniquement les demandes provenant d'un cloud privé virtuel (VPC) afin de restreindre l'accès aux données Amazon S3 à un réseau privé. Vous pouvez également configurer des paramètres de blocage de l'accès public personnalisés pour chaque point d'accès. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Le Compte AWS propriétaire ou le propriétaire du bucket doit mettre un site Web statique à la disposition du public

Avec S3, vous pouvez héberger un site web statique et autoriser tout le monde à consulter le contenu du site web, qui est hébergé à partir d'un compartiment S3.

Nous recommandons les outils suivants de gestion des accès pour ce cas d'utilisation :

- Amazon CloudFront — Cette solution vous permet d'héberger un site Web statique Amazon S3 accessible au public tout en continuant à bloquer tout accès public au contenu d'un compartiment. Si vous souhaitez conserver les quatre paramètres S3 Block Public Access activés et héberger un site Web statique S3, vous pouvez utiliser le contrôle CloudFront d'accès d'origine (OAC) d'Amazon. Amazon CloudFront fournit les fonctionnalités requises pour configurer un site Web statique sécurisé. En outre, les sites Web statiques Amazon S3 qui n'utilisent pas cette solution ne peuvent prendre en charge que les points de terminaison HTTP. CloudFront utilise le stockage durable d'Amazon S3 tout en fournissant des en-têtes de sécurité supplémentaires, tels que HTTPS. HTTPS accroît la sécurité en chiffrant une demande HTTP normale et en offrant une protection contre les cyberattaques courantes.

Pour plus d'informations, consultez Getting started with a secure static website in the Amazon CloudFront Developer Guide.

- Rendre votre compartiment Amazon S3 accessible publiquement : vous pouvez configurer un compartiment pour qu'il soit utilisé comme site web statique accessible publiquement.

  > **Warning**
  >
  > Cette méthode est déconseillée. Nous vous recommandons plutôt d'utiliser les sites Web statiques Amazon S3 dans le cadre d'Amazon CloudFront. Pour plus d'informations, consultez l'option précédente ou la section Démarrer avec un site web statique sécurisé.

  Pour créer un site Web statique Amazon S3, sans Amazon CloudFront, vous devez d'abord désactiver tous les paramètres de blocage de l'accès public. Lorsque vous rédigez la politique de compartiment pour votre site Web statique, veillez à autoriser uniquement des actions `s3:GetObject`, et non pas des autorisations `ListObject` ni `PutObject`. Cela permet de s'assurer que les utilisateurs ne peuvent pas voir tous les objets de votre compartiment ni ajouter leur propre contenu. Pour de plus amples informations, veuillez consulter Définition des autorisations pour l'accès au site web.

Le Compte AWS propriétaire ou le propriétaire du bucket souhaite rendre le contenu d'un bucket accessible au public

Lors de la création d'un compartiment Amazon S3, le paramètre Bloquer l'accès public est activé par défaut. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

Nous vous déconseillons d'autoriser l'accès public à votre compartiment. Toutefois, si vous devez l'autoriser pour un cas d'utilisation particulier, nous vous recommandons l'outil de gestion des accès suivant pour ce cas d'utilisation :

- Désactiver le paramètre Bloquer l'accès public : le propriétaire d'un compartiment peut autoriser les demandes non authentifiées adressées au compartiment. Par exemple, les demandes PUT Object non authentifiées sont permises lorsqu'un compartiment dispose d'une politique de compartiment publique ou lorsqu'une liste ACL de compartiment autorise l'accès public. Toutes les demandes non authentifiées sont faites par d'autres AWS utilisateurs arbitraires, ou même par des utilisateurs anonymes non authentifiés. Cet utilisateur est représenté ACLs par l'ID

`65a011a29cdf8ec533ec3d1ccaae921c` utilisateur canonique spécifique. Si un objet est chargé vers `WRITE` ou `FULL_CONTROL`, l'accès est uniquement accordé au groupe Tous les utilisateurs ou à l'utilisateur anonyme. Pour plus d'informations sur les politiques relatives aux compartiments publics et les listes de contrôle d'accès public (ACLs), consultezLa signification du mot « public ».

Le Compte AWS propriétaire ou le propriétaire du bucket a dépassé les limites de taille fixées par la politique d'accès

Les politiques de compartiment et les politiques basées sur l'identité ont une limite de taille de 20 Ko. Si vos exigences en matière d'autorisation d'accès sont complexes, vous risquez de dépasser cette limite.

Nous recommandons les outils de gestion des accès suivants pour ce cas d'utilisation :

- Points d'accès : utilisez des points d'accès si cela convient à votre cas d'utilisation. En ce qui concerne les points d'accès, chaque compartiment possède plusieurs points de terminaison réseau nommés, chacun ayant sa propre stratégie de point d'accès qui fonctionne avec la politique de compartiment sous-jacente. Toutefois, les points d'accès ne peuvent agir que sur des objets, et non sur des compartiments, et ne prennent pas en charge la réplication entre régions. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .
- Autorisations d'accès S3 : utilisez les autorisations d'accès S3, qui prennent en charge un très grand nombre d'autorisations donnant accès à des compartiments, à des préfixes ou à des objets. Pour de plus amples informations, veuillez consulter Bien démarrer avec les autorisations d'accès S3.

Le rôle de Compte AWS propriétaire ou d'administrateur souhaite accorder l'accès au bucket, au préfixe ou à l'objet directement aux utilisateurs ou aux groupes d'un annuaire d'entreprise

Au lieu de gérer les utilisateurs, les groupes et les rôles via AWS Identity and Access Management (IAM), vous pouvez y ajouter votre annuaire d' AWS IAM Identity Center entreprise. Pour plus d'informations, consultez En quoi consiste IAM Identity Center ?.

Après avoir ajouté votre annuaire d'entreprise à AWS IAM Identity Center, nous vous recommandons d'utiliser l'outil de gestion des accès suivant pour accorder aux identités d'annuaire d'entreprise l'accès à vos ressources S3 :

- Autorisations d'accès S3 : utilisez les autorisations d'accès S3, qui permettent d'accorder l'accès à des utilisateurs ou à des rôles issus de votre annuaire d'entreprise. Pour de plus amples informations, veuillez consulter Bien démarrer avec les autorisations d'accès S3.

Le Compte AWS propriétaire ou le propriétaire du compartiment souhaite autoriser le AWS CloudFront service à écrire CloudFront des journaux dans un compartiment S3

Nous recommandons l'outil de gestion des accès suivant pour ce cas d'utilisation :

- ACL du bucket — Le seul cas d'utilisation recommandé pour le bucket ACLs est d'accorder des autorisations à certains Services AWS, tels que le CloudFront `awslogsdelivery` compte Amazon. Lorsque vous créez ou mettez à jour une distribution et que vous activez la CloudFront journalisation, CloudFront met à jour l'ACL du bucket pour `awslogsdelivery` autoriser `FULL_CONTROL` le compte à écrire des journaux dans votre bucket. Pour plus d'informations, consultez la section Autorisations requises pour configurer la journalisation standard et pour accéder à vos fichiers journaux dans le manuel Amazon CloudFront Developer Guide. Si le compartiment qui stocke les journaux utilise le paramètre imposé par le propriétaire du compartiment pour désactiver la propriété des objets S3 ACLs, il CloudFront ne peut pas écrire de journaux dans le compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

En tant que propriétaire du compartiment, vous souhaitez conserver le contrôle total des objets ajoutés au compartiment par d'autres utilisateurs

Vous pouvez autoriser d'autres comptes à charger des objets dans votre compartiment en utilisant une politique de compartiment, un point d'accès ou des autorisations d'accès S3. Si vous avez accordé un accès intercompte à votre compartiment, vous pouvez vous assurer que tous les objets chargés dans votre compartiment restent sous votre contrôle total.

Nous recommandons l'outil de gestion des accès suivant pour ce cas d'utilisation :

- Propriété d'objets : conservez le paramètre Propriété d'objets au niveau du compartiment sur le paramètre par défaut Propriétaire du compartiment appliqué.

Résolution des problèmes de gestion d'accès

Les ressources suivantes peuvent vous aider à résoudre les problèmes de gestion d'accès S3 :

Résolution des erreurs d'accès refusé (403 Forbidden)

Si vous rencontrez des problèmes de refus d'accès, vérifiez les paramètres au niveau du compte et au niveau du compartiment. Vérifiez également la fonctionnalité de gestion des accès que vous utilisez pour accorder l'accès afin de vous assurer que la politique, le paramètre ou la configuration sont corrects. Pour plus d'informations sur les causes courantes des erreurs d'accès refusé (403 Forbidden) dans Amazon S3, consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3.

Analyseur d'accès IAM pour S3

Si vous ne souhaitez rendre aucune de vos ressources accessible au public, ou si vous souhaitez limiter l'accès public à vos ressources, vous pouvez utiliser l'analyseur d'accès IAM pour S3. Sur la console Amazon S3, utilisez IAM Access Analyzer for S3 pour examiner tous les compartiments dotés de listes de contrôle d'accès aux compartiments (ACLs), de politiques de compartiment ou de politiques de point d'accès accordant un accès public ou partagé. IAM Access Analyzer for S3 vous avertit de la présence de compartiments configurés pour autoriser l'accès à toute personne sur Internet ou autre Comptes AWS, y compris Comptes AWS en dehors de votre organisation. Pour chaque compartiment public ou partagé, vous recevez des résultats qui signalent la source et le niveau d'accès public ou partagé.

Dans l'analyseur d'accès IAM pour S3, vous pouvez bloquer tout accès public à un compartiment en une seule action. Nous vous recommandons de bloquer tout accès public à vos compartiments, sauf si vous avez besoin d'un accès public pour répondre à un cas d'utilisation spécifique. Avant de bloquer tout accès public, assurez-vous que vos applications continueront à fonctionner correctement sans cet accès. Pour de plus amples informations, veuillez consulter Blocage de l'accès public à votre stockage Amazon S3.

Vous pouvez également passer en revue les paramètres d'autorisation au niveau des compartiments afin de configurer des niveaux détaillés d'accès. Pour les cas d'utilisation spécifiques et vérifiés nécessitant un accès public ou partagé, vous pouvez confirmer et enregistrer votre intention de maintenir le niveau d'accès public ou partagé en archivant les résultats pour le compartiment. Vous pouvez revisiter et modifier ces configurations de compartiments à tout moment. Vous pouvez également télécharger vos résultats sous forme de rapport CSV à des fins d'audit.

L'analyseur d'accès IAM pour S3 est disponible gratuitement sur la console Amazon S3. L'analyseur d'accès IAM pour S3 est optimisé par l'analyseur d'accès IAM d' AWS Identity and Access Management (IAM). Pour utiliser l'analyseur d'accès IAM pour S3 dans la console Amazon S3, vous

devez accéder à la console IAM et créer un analyseur au niveau du compte dans l'analyseur d'accès IAM pour chaque région.

Pour plus d'informations sur l'analyseur d'accès IAM pour S3, consultez Examen de l'accès aux compartiments à l'aide de l'analyseur d'accès IAM pour S3.

Journalisation et surveillance

La surveillance est un élément clé pour assurer la fiabilité, la disponibilité et les performances de vos solutions Amazon S3 pour vous permettre de déboguer plus facilement un échec d'accès. La journalisation peut fournir un aperçu des erreurs reçues par les utilisateurs, ainsi que du moment et des demandes qui leur sont adressées. AWS fournit plusieurs outils pour surveiller vos ressources Amazon S3, tels que les suivants :

- AWS CloudTrail
- Journaux d'accès Amazon S3
- AWS Trusted Advisor
- Amazon CloudWatch

Pour de plus amples informations, veuillez consulter Journalisation et surveillance dans Amazon S3.

Gestion des identités et des accès pour Amazon S3

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (disposant des autorisations requises) à utiliser des ressources Amazon S3. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Rubriques

- Public ciblé
- Authentification par des identités
- Gestion des accès à l'aide de politiques
- Fonctionnement d'Amazon S3 avec IAM
- Comment Amazon S3 autorise une demande
- Autorisations requises pour les opérations d'API Amazon S3
- Politiques, stratégies et autorisations dans Amazon S3
- Politiques de compartiment pour Amazon S3
- Politiques basées sur l'identité pour Amazon S3
- Procédures détaillées qui utilisent des politiques pour gérer l'accès à vos ressources Amazon S3
- Utilisation des rôles liés à un service pour Amazon S3 Storage Lens
- Résolution des problèmes d'identité et d'accès Amazon S3
- AWS politiques gérées pour Amazon S3

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Amazon S3.

Utilisateur du service : si vous utilisez le service Amazon S3 pour accomplir votre tâche, l'administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Vous pourrez avoir besoin d'autorisations supplémentaires si vous utilisez davantage de fonctionnalités Amazon S3. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne parvenez pas à accéder à une fonctionnalité dans Amazon S3, consultez Résolution des problèmes d'identité et d'accès Amazon S3.

Administrateur du service : si vous êtes responsable des ressources Amazon S3 dans votre entreprise, vous bénéficiez probablement d'un accès total à ce service. C'est à vous de déterminer les fonctionnalités et les ressources Amazon S3 auxquelles les utilisateurs des services doivent avoir accès. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour

comprendre les concepts de base d'IAM. Pour découvrir la façon dont votre entreprise peut utiliser IAM avec Amazon S3, consultez Fonctionnement d'Amazon S3 avec IAM.

Administrateur IAM : si vous êtes un administrateur IAM, vous souhaiterez peut-être obtenir des informations sur la façon dont vous pouvez écrire des politiques pour gérer l'accès à Amazon S3. Pour afficher des exemples de politiques basées sur l'identité Amazon S3 que vous pouvez utiliser dans IAM, consultez Politiques basées sur l'identité pour Amazon S3.

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 (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles 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. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, 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 au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une

rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. 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 au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.

- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser 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.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance.

Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des 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 est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

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.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. 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.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources 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

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.
- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. 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.

Fonctionnement d'Amazon S3 avec IAM

Avant d'utiliser IAM pour gérer l'accès à Amazon S3, découvrez les fonctionnalités IAM qui peuvent être utilisées avec Amazon S3.

Fonctionnalités IAM que vous pouvez utiliser avec Amazon S3

Fonctionnalité IAM	Prise en charge d'Amazon S3
Politiques basées sur l'identité	Oui
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition de politique (spécifiques au service)	Oui
ACLs	Oui
ABAC (identifications dans les politiques)	Partielle
Informations d'identification temporaires	Oui
Transmission des sessions d'accès (FAS)	Oui
Rôles de service	Oui
Rôles liés à un service	Partielle

Pour obtenir une vue d'ensemble de la façon dont Amazon S3 et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Politiques basées sur l'identité pour Amazon S3

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. 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. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. 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.

Exemples de politiques basées sur l'identité pour Amazon S3

Pour voir des exemples de politiques Amazon S3 basées sur l'identité, consultez Politiques basées sur l'identité pour Amazon S3.

Politiques basées sur les ressources au sein d'Amazon S3

Prend en charge les politiques basées sur les ressources : oui

Les politiques basées sur les ressources 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. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Le service Amazon S3 prend en charge les politiques de compartiment, les stratégies de points d'accès et les autorisations d'accès S3 :

- Les politiques de compartiment sont des politiques basées sur les ressources. Elles sont associées à un compartiment Amazon S3. Une politique de compartiment désigne les principaux autorisés à effectuer des actions au niveau de ce compartiment.
- Les stratégies de points d'accès sont des politiques basées sur les ressources. Elles sont évaluées conjointement avec la politique de compartiment sous-jacente.
- Les autorisations d'accès S3 fournissent un modèle simplifié pour définir les autorisations d'accès aux données dans Amazon S3 par préfixe, compartiment ou objet. Pour plus d'informations sur les autorisations d'accès S3, consultez Gestion de l'accès avec les autorisations d'accès S3.

Principaux pour les politiques de compartiment

L'élément `Principal` spécifie l'utilisateur, le compte, le service ou une autre entité qui a accès ou non à une ressource. Voici quelques exemples de spécification de `Principal`. Pour plus d'informations, consultez Principal dans le Guide de l'utilisateur IAM.

Accorder des autorisations à un Compte AWS

Pour accorder des autorisations à un Compte AWS, identifiez le compte en utilisant le format suivant.

```
"AWS":"account-ARN"
```

Voici quelques exemples.

```
"Principal":{"AWS":"arn:aws:iam::AccountIDWithoutHyphens:root"}
```

```
"Principal":{"AWS":
["arn:aws:iam::AccountID1WithoutHyphens:root","arn:aws:iam::AccountID2WithoutHyphens:root"]}
```

> **Note**
>
> Les exemples ci-dessus accordent des autorisations à l'utilisateur root, qui les délègue au niveau du compte. Cependant, des politiques IAM sont toujours requises pour les rôles et les utilisateurs spécifiques du compte.

Octroyer des autorisations à un utilisateur IAM

Pour accorder une autorisation à un utilisateur IAM de votre compte, vous devez fournir une paire de nom-valeur `"AWS":"user-ARN"`.

```
"Principal":{"AWS":"arn:aws:iam::account-number-without-hyphens:user/username"}
```

Pour des exemples détaillés fournissant des step-by-step instructions, reportez-vous aux sections Exemple 1 : propriétaire d'un compartiment accordant à ses utilisateurs des autorisations sur un compartiment etExemple 3 : propriétaire d'un compartiment accordant des autorisations sur des objets qu'il ne possède pas.

> **Note**
>
> Si une identité IAM est supprimée après la mise à jour de votre politique de compartiment, la politique de compartiment affichera un identifiant unique dans l'élément principal au lieu d'un ARN. Ces informations uniques ne IDs sont jamais réutilisées. Vous pouvez donc supprimer en toute sécurité les principaux associés à des identifiants uniques de toutes vos déclarations de politique. Pour plus d'informations sur les identifiants uniques, consultez Identificateurs IAM dans le Guide de l'utilisateur IAM.

Octroyer des autorisations anonymes

> **Warning**
>
> Soyez vigilant lorsque vous accordez un accès anonyme à votre compartiment Amazon S3. Lorsque vous accordez un accès anonyme, tout le monde peut accéder à votre compartiment. Nous vous recommandons vivement de ne jamais accorder un type d'accès en écriture anonyme quel qu'il soit à votre compartiment S3.

Pour accorder l'autorisation à tout le monde (on parle aussi d'accès anonyme), définissez le caractère générique `"*"` en tant que valeur `Principal`. Par exemple, si vous configurez votre compartiment en tant que site Web, vous voulez que tous les objets dans le compartiment soit accessibles publiquement.

```
"Principal":"*"
```

```
"Principal":{"AWS":"*"}
```

L'utilisation `"Principal": "*"` avec `Allow` effet dans le cadre d'une politique basée sur les ressources permet à quiconque, même s'il n'est pas connecté AWS, d'accéder à votre ressource.

L'utilisation de l'interface `"Principal" : { "AWS" : "*" }` avec un effet `Allow` dans une politique basée sur les ressources permet à n'importe quel utilisateur racine, utilisateur IAM, séance à rôle supposé ou utilisateur fédéré dans n'importe quel compte de la même partition d'accéder à votre ressource.

Pour les utilisateurs anonymes, ces deux méthodes sont équivalentes. Pour plus d'informations, consultez Tous les principaux dans le Guide de l'utilisateur IAM.

Vous ne pouvez pas utiliser un caractère générique pour une correspondance à une partie d'un nom ou d'un ARN principal.

> **Important**
>
> Dans les politiques de contrôle d' AWS accès, les principes « * » et {»AWS« : « *"} se comportent de manière identique.

Restriction des autorisations sur les ressources

Vous pouvez également utiliser la politique sur les ressources pour restreindre l'accès aux ressources qui seraient autrement accessibles aux principaux IAM. Utilisez une instruction `Deny` pour empêcher l'accès.

L'exemple suivant bloque l'accès si aucun protocole de transport sécurisé n'est utilisé :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyBucketAccessIfSTPNotUsed",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      }
    }
  ]
}
```

Au lieu de tenter de refuser l'accès à des comptes ou des principaux spécifiques selon cette méthode, l'utilisation de `"Principal": "*"` de sorte que cette restriction s'applique à tout le monde est une bonne pratique pour cette politique.

Exiger un accès via CloudFront URLs

Vous pouvez demander à vos utilisateurs d'accéder à votre contenu Amazon S3 uniquement en utilisant CloudFront URLs plutôt qu'Amazon S3 URLs. Pour ce faire, créez un contrôle CloudFront d'accès à l'origine (OAC). Modifiez ensuite les autorisations au niveau de vos données S3. Dans votre politique de compartiment, vous pouvez définir le CloudFront rôle principal comme suit :

```
"Principal":{"Service":"cloudfront.amazonaws.com"}
```

Utilisez un `Condition` élément de la politique CloudFront pour autoriser l'accès au compartiment uniquement lorsque la demande provient de la CloudFront distribution contenant l'origine S3.

```
       "Condition": {
          "StringEquals": {
             "AWS:SourceArn":
 "arn:aws:cloudfront::111122223333:distribution/CloudFront-distribution-ID"
          }
       }
```

Pour plus d'informations sur l'obligation d'accéder à S3 via CloudFront URLs, consultez Restreindre l'accès à une origine Amazon Simple Storage Service dans le manuel Amazon CloudFront Developer Guide. Pour plus d'informations sur les avantages en matière de sécurité et de confidentialité liés à l'utilisation d'Amazon CloudFront, consultez Configuration de l'accès sécurisé et restriction de l'accès au contenu.

Exemples de politiques basées sur les ressources pour Amazon S3

- Pour obtenir des exemples de politiques de compartiment Amazon S3, consultez Politiques de compartiment pour Amazon S3.
- Pour consulter des exemples de stratégies de points d'accès, consultez Configuration des politiques IAM pour l'utilisation des points d'accès.

Actions de politique pour Amazon S3

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. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations

nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Vous trouverez ci-dessous les différents types de relations de mappage entre les opérations de l'API S3 et les actions de politiques requises.

- One-to-one mappage portant le même nom. Par exemple, pour utiliser l'opération d'API `PutBucketPolicy`, l'action de politique `s3:PutBucketPolicy` est requise.
- One-to-one mappage avec des noms différents. Par exemple, pour utiliser l'opération d'API `ListObjectsV2`, l'action de politique `s3:ListBucket` est requise.
- One-to-many cartographie. Par exemple, pour utiliser l'opération d'API `HeadObject`, `s3:GetObject` est requis. De même, lorsque vous utilisez le verrouillage d'objet S3 et que vous souhaitez obtenir le statut de conservation légale d'un objet ou les paramètres de rétention d'un objet, les actions de politique `s3:GetObjectLegalHold` ou `s3:GetObjectRetention` correspondantes sont également requises avant de pouvoir utiliser l'opération d'API `HeadObject`.
- Many-to-one cartographie. Par exemple, pour utiliser les opérations d'API `ListObjectsV2` ou `HeadBucket`, l'action de politique `s3:ListBucket` est requise.

Pour afficher la liste des actions Amazon S3 que vous pouvez utilisez dans les politiques, consultez Actions définies par Amazon S3 dans la Référence de l'autorisation de service. Pour obtenir la liste des opérations d'API Amazon S3, consultez Actions d'API Amazon S3 dans la Référence d'API Amazon Simple Storage Service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Les actions de politique dans Amazon S3 utilisent le préfixe suivant avant l'action :

```
s3
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "s3:action1",
```

```
      "s3:action2"
         ]
```

Opérations de compartiment

Les opérations de compartiment sont des opérations d'API S3 qui opèrent sur le type de ressource du compartiment. Par exemple, `CreateBucket`, `ListObjectsV2` et `PutBucketPolicy`. Les actions de politique S3 pour les opérations de compartiment nécessitent que l'élément `Resource` des politiques de compartiment ou des politiques basées sur l'identité IAM soit l'identifiant Amazon Resource Name (ARN) du type de compartiment S3 dans l'exemple de format suivant.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
```

La politique de compartiment suivante accorde à l'utilisateur *Akua* titulaire du compte *12345678901* l'autorisation `s3:ListBucket` d'effectuer l'opération d'API ListObjectsV2 et de répertorier les objets dans un compartiment S3.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
        }
    ]
}
```

Opérations relatives aux compartiments dans les politiques relatives aux points d'accès pour les compartiments à usage général

Les autorisations accordées dans un point d'accès pour la politique des buckets à usage général ne sont effectives que si le bucket sous-jacent autorise les mêmes autorisations. Lorsque vous utilisez des points d'accès S3, vous devez déléguer le contrôle d'accès du compartiment au point d'accès ou ajouter les mêmes autorisations dans les stratégies du point d'accès à la politique du compartiment sous-jacent. Pour de plus amples informations, veuillez consulter Configuration des politiques IAM pour l'utilisation des points d'accès. Dans les stratégies de point d'accès, les actions de politique S3 pour les opérations de compartiment nécessitent que vous utilisiez l'ARN du point d'accès pour l'élément `Resource` au format suivant.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

La stratégie de point d'accès suivante accorde à l'utilisateur *Akua* titulaire du compte *12345678901* l'autorisation `s3:ListBucket` d'effectuer l'opération d'API ListObjectsV2 via le point d'accès S3 nommé *example-access-point*. Cette autorisation permet à *Akua* de répertorier les objets dans le compartiment associé à *example-access-point*.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access
 point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-
access-point"
        }
    ]
}
```

> **Note**
>
> Toutes les opérations liées aux compartiments ne sont pas prises en charge par des points d'accès pour les compartiments à usage général. Pour de plus amples informations, veuillez consulter Compatibilité des points d'accès avec les opérations S3.

Opérations relatives aux compartiments dans les politiques relatives aux points d'accès aux compartiments d'annuaire

Les autorisations accordées dans une politique de points d'accès pour les compartiments d'annuaire ne sont efficaces que si le compartiment sous-jacent autorise les mêmes autorisations. Lorsque vous utilisez des points d'accès S3, vous devez déléguer le contrôle d'accès du compartiment au point d'accès ou ajouter les mêmes autorisations dans les stratégies du point d'accès à la politique du compartiment sous-jacent. Pour de plus amples informations, veuillez consulter Configuration des politiques IAM pour l'utilisation des points d'accès pour les compartiments d'annuaire. Dans les stratégies de point d'accès, les actions de politique S3 pour les opérations de compartiment nécessitent que vous utilisiez l'ARN du point d'accès pour l'élément `Resource` au format suivant.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

La politique de point d'accès suivante accorde *Akua* à l'utilisateur titulaire *12345678901* du compte l'`s3:ListBucket`autorisation d'effectuer l'opération d'ListObjectsV2API via le point d'accès nommé*example-access-point--usw2-az1--xa-s3*. Cette autorisation permet à *Akua* de répertorier les objets dans le compartiment associé à *example-access-point--usw2-az1--xa-s3*.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to list objects in the bucket through access
 point",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:ListBucket"
            ],
            "Resource": "arn:aws:s3express:us-
west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
        }
    ]
}
```

> **Note**
>
> Les opérations de compartiment ne sont pas toutes prises en charge par les points d'accès pour les compartiments de répertoire. Pour de plus amples informations, veuillez consulter Opérations sur les objets pour les points d'accès aux compartiments de répertoire.

Opérations d'objet

Les opérations d'objet sont des opérations d'API S3 qui agissent sur le type de ressource de l'objet. Par exemple, `GetObject`, `PutObject` et `DeleteObject`. Les actions de politique S3 pour les opérations d'objet nécessitent que l'élément `Resource` des politiques soit l'ARN de l'objet S3 dans les exemples de formats suivants.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/*"
```

> **Note**
>
> L'ARN de l'objet doit contenir une barre oblique après le nom du compartiment, comme indiqué dans les exemples précédents.

La politique de compartiment suivante accorde à l'utilisateur (*Akua*) du compte *12345678901* l'autorisation `s3:PutObject`. Cette autorisation permet à *Akua* d'utiliser l'opération d'API PutObject pour charger des objets dans le compartiment S3 nommé *amzn-s3-demo-bucket*.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to upload objects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Akua"
            },
            "Action": [
            "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
        }
    ]
}
```

Opérations d'objet dans les stratégies de point d'accès

Lorsque vous utilisez des points d'accès S3 pour contrôler l'accès aux opérations d'objet, vous pouvez opter pour des stratégies de point d'accès. Lorsque vous utilisez des stratégies de point d'accès, les actions de politique S3 pour les opérations d'objet nécessitent que vous utilisiez l'ARN du point d'accès pour l'élément `Resource` au format suivant :`arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource`. Pour les opérations d'objet qui utilisent des points d'accès, vous devez inclure la valeur `/object/` après l'ARN complet du point d'accès dans l'élément `Resource`. Voici quelques exemples.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/
*"
```

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/
object/prefix/*"
```

La stratégie de point d'accès suivante accorde à l'utilisateur *Akua* titulaire du compte *12345678901* l'autorisation `s3:GetObject`. Cette autorisation permet à *Akua* d'effectuer l'opération d'API GetObject via le point d'accès nommé *example-access-point* sur tous les objets du compartiment associé à ce point d'accès.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": [
            "s3:GetObject"
            ],
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point/object/*"
        }
    ]
}
```

> **Note**
>
> Les opérations d'objet ne sont pas toutes prises en charge par les points d'accès. Pour de plus amples informations, veuillez consulter Compatibilité des points d'accès avec les opérations S3.

Opérations sur les objets dans les politiques relatives aux points d'accès aux compartiments d'annuaire

Lorsque vous utilisez des points d'accès pour des compartiments de répertoire afin de contrôler l'accès aux opérations sur les objets, vous pouvez utiliser des politiques de point d'accès. Lorsque vous utilisez des stratégies de point d'accès, les actions de politique S3 pour les opérations d'objet nécessitent que vous utilisiez l'ARN du point d'accès pour l'élément `Resource` au format suivant :`arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource`. Pour les opérations d'objet qui utilisent des points d'accès, vous devez inclure la valeur `/object/` après l'ARN complet du point d'accès dans l'élément `Resource`. Voici quelques exemples.

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
```

```
"Resource": "arn:aws:s3express:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/prefix/*"
```

La stratégie de point d'accès suivante accorde à l'utilisateur *Akua* titulaire du compte *12345678901* l'autorisation `s3:GetObject`. Cette autorisation permet à *Akua* d'effectuer l'opération d'API GetObject via le point d'accès nommé *example-access-point--usw2-az1--xa-s3* sur tous les objets du compartiment associé à ce point d'accès.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow Akua to get objects through access point",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::12345678901:user/Akua"
            },
            "Action": "s3express:CreateSession","s3:GetObject"
            "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3/object/*"
        }
    ]
}
```

> **Note**
>
> Les opérations sur les objets ne sont pas toutes prises en charge par les points d'accès pour les compartiments de répertoire. Pour de plus amples informations, veuillez consulter Opérations sur les objets pour les points d'accès aux compartiments de répertoire.

Point d'accès pour les opérations de godet à usage général

Les opérations de point d'accès sont des opérations d'API S3 qui agissent sur le type de ressource `accesspoint`. Par exemple, `CreateAccessPoint`, `DeleteAccessPoint` et `GetAccessPointPolicy`. Les actions de politique S3 pour les opérations de point d'accès ne

peuvent être utilisées que dans les politiques basées sur l'identité IAM, et non dans les politiques de compartiment ou les stratégies de point d'accès. Les opérations de points d'accès nécessitent que l'élément `Resource` soit l'ARN du point d'accès dans l'exemple de format suivant.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point"
```

La politique basée sur l'identité IAM suivante accorde l'autorisation `s3:GetAccessPointPolicy` d'effectuer l'opération d'API GetAccessPointPolicy au niveau du point d'accès S3 nommé *example-access-point*.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of
 access point example-access-point",
            "Effect": "Allow",
            "Action": [
            "s3:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-
point"
        }
    ]
}
```

Lorsque vous utilisez des points d'accès, pour contrôler l'accès aux opérations de compartiment, consultez Opérations relatives aux compartiments dans les politiques relatives aux points d'accès pour les compartiments à usage général et, pour contrôler l'accès aux opérations d'objet, consultez Opérations d'objet dans les stratégies de point d'accès. Pour plus d'informations sur la configuration de stratégies de point d'accès, consultez Configuration des politiques IAM pour l'utilisation des points d'accès.

Point d'accès pour les opérations relatives aux buckets d'annuaires

Les opérations de point d'accès pour les compartiments d'annuaire sont des opérations d'API S3 qui opèrent sur le type de `accesspoint` ressource. Par exemple, `CreateAccessPoint`,

`DeleteAccessPoint` et `GetAccessPointPolicy`. Les actions de politique S3 pour les opérations de point d'accès ne peuvent être utilisées que dans les politiques basées sur l'identité IAM, et non dans les politiques de compartiment ou les stratégies de point d'accès. Les points d'accès pour les opérations de compartiments de répertoire nécessitent que l'`Resource`élément soit l'ARN du point d'accès dans l'exemple de format suivant.

```
"Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/example-access-point--usw2-az1--xa-s3"
```

La politique basée sur l'identité IAM suivante accorde l'`s3express:GetAccessPointPolicy`autorisation d'effectuer l'opération d'GetAccessPointPolicyAPI sur le point d'accès nommé. *`example-access-point--usw2-az1--xa-s3`*

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant permission to retrieve the access point policy of
 access point example-access-point--usw2-az1--xa-s3",
            "Effect": "Allow",
            "Action": [
            "s3express:CreateSession","s3express:GetAccessPointPolicy"
            ],
            "Resource": "arn:aws:s3:*:123456789012:accesspoint/example-access-
point--usw2-az1--xa-s3"
        }
    ]
}
```

La politique basée sur l'identité IAM suivante accorde l'`s3express:CreateAccessPoint`autorisation de créer des points d'accès pour les buckets d'annuaire.

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

```
    "Statement": [
        {
            "Sid": "Grant CreateAccessPoint.",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint""Effect": "Allow",
            "Resource": "*"
        }
    ]
}
```

La politique basée sur l'identité IAM suivante accorde l'`s3express:PutAccessPointScope`autorisation de créer une étendue de point d'accès pour les points d'accès pour les compartiments d'annuaire.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Grant PutAccessPointScope",
            "Principal": "*",
            "Action": "s3express:CreateSession",
            "s3express:CreateAccessPoint",
            "S3Express:PutAccessPointScope""Effect": "Allow",
            "Resource": "*",
        }
    ]
}
```

Lorsque vous utilisez des points d'accès pour les compartiments de répertoire afin de contrôler l'accès aux opérations des compartiments, voir Opérations relatives aux compartiments dans les politiques relatives aux points d'accès aux compartiments d'annuaire ; pour contrôler l'accès aux opérations sur les objets, voirOpérations sur les objets dans les politiques relatives aux points d'accès aux compartiments d'annuaire. Pour plus d'informations sur la configuration des points d'accès pour les politiques de compartiments d'annuaire, consultezConfiguration des politiques IAM pour l'utilisation des points d'accès pour les compartiments d'annuaire.

Opérations de point d'accès Object Lambda

Amazon S3 Object Lambda vous donne la possibilité d'ajouter votre propre code aux requêtes Amazon S3 `GET`, `LIST` et `HEAD` afin de modifier et de traiter les données lorsqu'elles sont renvoyées vers une application. Vous pouvez effectuer des demandes via un point d'accès Object Lambda, ce qui fonctionne de la même manière que les demandes via d'autres points d'accès. Pour de plus amples informations, veuillez consulter Transformation d'objets avec S3 Object Lambda.

Pour plus d'informations sur la configuration de politiques pour les opérations de point d'accès Object Lambda, consultez Configuration des politiques IAM pour les points d'accès Object Lambda.

Opérations de point d'accès multi-régions

Les points d'accès multi-régions Amazon S3 fournissent un point de terminaison global que les applications peuvent utiliser pour traiter les demandes provenant de compartiments S3 situés dans plusieurs Région AWS. Vous pouvez utiliser des points d'accès multi-régions pour créer des applications multi-régions avec la même architecture que celle utilisée dans une seule région, puis exécuter ces applications partout dans le monde. Pour de plus amples informations, veuillez consulter Gestion du trafic multirégional avec des points d'accès multirégionaux.

Pour plus d'informations sur la configuration de stratégies pour les opérations de points d'accès multi-régions, consultez Exemples de politique de point d'accès multi-régions.

Opérations relatives aux tâches par lots

Les opérations relatives aux tâches par lots (opérations par lot) sont des opérations d'API S3 qui agissent sur le type de ressource job. Par exemple : `DescribeJob` et `CreateJob`. Les actions de politique S3 pour les opérations relatives aux tâches par lots ne peuvent être utilisées que dans les politiques basées sur l'identité IAM, et non dans les politiques de compartiment. En outre, les opérations relatives aux tâches par lots nécessitent que l'élément `Resource` des politiques basées sur l'identité IAM soit l'ARN de l'élément `job` dans l'exemple de format suivant.

```
"Resource": "arn:aws:s3:*:123456789012:job/*"
```

La politique basée sur l'identité IAM suivante accorde l'`s3:DescribeJob`autorisation d'effectuer l'opération d'DescribeJobAPI sur le job S3 Batch Operations nommé. *`example-job`*

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowDescribingBatchOperationJob",
            "Effect": "Allow",
            "Action": [
            "s3:DescribeJob"
            ],
            "Resource": "arn:aws:s3:*:111122223333:job/example-job"
        }
    ]
}
```

Opérations de configuration S3 Storage Lens

Pour plus d'informations sur les opérations de configuration S3 Storage Lens, consultez Définition d'autorisations Amazon S3 Storage Lens.

Opérations de compte

Les opérations de compte sont des opérations d'API S3 qui agissent au niveau du compte. Par exemple, `GetPublicAccessBlock` (pour le compte). Le compte n'est pas un type de ressource défini par Amazon S3. Les actions de politique S3 pour les opérations de compte ne peuvent être utilisées que dans les politiques basées sur l'identité IAM, et non dans les politiques de compartiment. En outre, les opérations de compte nécessitent que l'élément `Resource` des politiques basées sur l'identité IAM soit `"*"`.

La politique basée sur l'identité IAM suivante accorde l'autorisation `s3:GetAccountPublicAccessBlock` d'effectuer l'opération d'API GetPublicAccessBlock au niveau du compte et de récupérer les paramètres de blocage de l'accès public au niveau du compte.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"AllowRetrievingTheAccountLevelPublicAccessBlockSettings",
         "Effect":"Allow",
         "Action":[
```

```
            "s3:GetAccountPublicAccessBlock"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Exemples de politiques pour Amazon S3

- Pour voir des exemples de politiques Amazon S3 basées sur l'identité, consultez Politiques basées sur l'identité pour Amazon S3.
- Pour afficher des exemples de politiques basées sur les ressources Amazon S3, consultez Politiques de compartiment pour Amazon S3 et Configuration des politiques IAM pour l'utilisation des points d'accès.

Ressources de politique pour Amazon S3

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. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Certaines actions d'API Amazon S3 prennent en charge plusieurs ressources. Par exemple, sachant que `s3:GetObject` accède à *`example-resource-1`* et à *`example-resource-2`*, un principal

doit disposer des autorisations d'accès à ces deux ressources. Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules, comme indiqué dans l'exemple suivant.

```
"Resource": [
      "example-resource-1",
      "example-resource-2"
```

Dans Amazon S3, les ressources sont les compartiments, les objets, les points d'accès ou les tâches. Dans une politique, utilisez l'Amazon Resource Name (ARN) du compartiment, de l'objet, du point d'accès ou de la tâche pour identifier la ressource.

Pour consulter la liste complète des types de ressources Amazon S3 et de leurs caractéristiques ARNs, consultez la section Ressources définies par Amazon S3 dans le Service Authorization Reference. Pour savoir les actions avec lesquelles vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par Amazon S3.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Caractères génériques dans la ressource ARNs

Vous pouvez utiliser des caractères génériques dans l'ARN d'une ressource. Vous pouvez utiliser des caractères génériques (* et ?) dans n'importe quel segment d'ARN (parties séparées par des signes deux-points). Un astérisque (*) représente n'importe quelle combinaison de zéro ou de plusieurs caractères, et un point d'interrogation (?) représente un seul caractère quelconque. Vous pouvez utiliser plusieurs caractères * ou ? dans chaque segment. Toutefois, un caractère générique ne peut pas couvrir des segments.

- L'ARN suivant utilise le caractère générique * dans la partie `relative-ID` de l'ARN pour identifier tous les objets du compartiment *amzn-s3-demo-bucket*.

  ```
  arn:aws:s3:::amzn-s3-demo-bucket/*
  ```

- L'ARN suivant utilise * pour indiquer tous les compartiments et tous les objets Amazon S3.

  ```
  arn:aws:s3:::*
  ```

- L'ARN suivant utilise les deux caractères génériques, * et ?, dans la partie `relative-ID`. Cet ARN identifie tous les objets des compartiments, par exemple *amzn-s3-demo-*

example1bucket, *amzn-s3-demo-example2bucket*, *amzn-s3-demo-example3bucket*, etc.

```
arn:aws:s3:::amzn-s3-demo-example?bucket/*
```

Variables de politique pour les ressources ARNs

Vous pouvez utiliser des variables de politique dans Amazon S3 ARNs. Lors de l'évaluation de la politique, ces variables prédéfinies sont remplacées par leurs valeurs correspondantes. Supposons que vous organisiez votre compartiment comme un ensemble de dossiers, avec un dossier pour chacun de vos utilisateurs. Le nom de dossier est le même que le nom d'utilisateur. Pour octroyer aux utilisateurs des autorisations à leurs dossiers, vous pouvez spécifier une variable de stratégie dans l'ARN de la ressource :

```
arn:aws:s3:::bucket_name/developers/${aws:username}/
```

Lors de l'exécution, quand la politique est évaluée, la variable `${aws:username}` dans l'ARN de la ressource est remplacée par le nom de l'utilisateur effectuant la demande.

Exemples de politiques pour Amazon S3

- Pour voir des exemples de politiques Amazon S3 basées sur l'identité, consultez Politiques basées sur l'identité pour Amazon S3.
- Pour afficher des exemples de politiques basées sur les ressources Amazon S3, consultez Politiques de compartiment pour Amazon S3 et Configuration des politiques IAM pour l'utilisation des points d'accès.

Clés de condition de politique pour Amazon S3

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` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. 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.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR` opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. 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.

Chaque clé de condition Amazon S3 est mappée à l'en-tête de demande du même nom autorisé par l'API sur lequel la condition peut être définie. Les clés de condition spécifiques à Amazon S3 dictent le comportement des en-têtes de demande du même nom. Par exemple, la clé de condition `s3:VersionId` utilisée pour octroyer l'autorisation conditionnelle pour `s3:GetObjectVersion`
définit le comportement du paramètre de requête `versionId` que vous définissez dans une demande GET Object.

Pour afficher la liste des clés de condition Amazon S3, consultez Clés de condition pour Amazon S3 dans la Référence de l'autorisation de service. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, consultez Actions définies par Amazon S3.

Exemple : Restreindre les chargements aux objets avec une classe de stockage spécifique

Supposons que le compte A, représenté par l'ID de compte *`123456789012`*, possède un compartiment. L'administrateur du compte A souhaite restreindre *`Dave`*un utilisateur du compte A, afin que *`Dave`* ne puisse charger des objets dans le compartiment que si l'objet est stocké dans la classe de stockage `STANDARD_IA`. Pour restreindre les chargements d'objets vers une classe de stockage spécifique, l'administrateur de compte A peut utiliser la clé de condition `s3:x-amz-storage-class`, comme illustré dans l'exemple de politique de compartiment suivant.

JSON

```
{
                "Version": "2012-10-17",
                "Statement": [
                  {
                    "Sid": "statement1",
                    "Effect": "Allow",
                    "Principal": {
                      "AWS": "arn:aws:iam::123456789012:user/Dave"
                    },
                    "Action": "s3:PutObject",
                    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                    "Condition": {
                      "StringEquals": {
                        "s3:x-amz-storage-class": [
                          "STANDARD_IA"
                        ]
                      }
                    }
                  }
                ]
            }
```

Dans l'exemple, le bloc `Condition` spécifie la condition `StringEquals` qui est appliquée à la paire clé-valeur spécifiée, `"s3:x-amz-acl":["public-read"]`. Un jeu de clés prédéfinis peut être utilisé pour exprimer une condition. L'exemple utilise la clé de condition `s3:x-amz-acl`. Cette condition exige que l'utilisateur inclue l'en-tête `x-amz-acl` avec la valeur `public-read` dans chaque demande `PutObject`.

Exemples de politiques pour Amazon S3

- Pour voir des exemples de politiques Amazon S3 basées sur l'identité, consultez Politiques basées sur l'identité pour Amazon S3.
- Pour afficher des exemples de politiques basées sur les ressources Amazon S3, consultez Politiques de compartiment pour Amazon S3 et Configuration des politiques IAM pour l'utilisation des points d'accès.

ACLs dans Amazon S3

Supports ACLs : Oui

Dans Amazon S3, les listes de contrôle d'accès (ACLs) contrôlent les Comptes AWS personnes autorisées à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

> **Important**
>
> La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs.

Pour plus d'informations sur l'utilisation ACLs pour contrôler l'accès dans Amazon S3, consultezGérer l'accès avec ACLs.

ABAC avec Amazon S3

Prend en charge ABAC (identifications dans les politiques) : partiellement

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

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 les ressources qui prennent en charge l'ABAC dans Amazon S3, consultez la section Utilisation de balises pour le contrôle d'accès basé sur les attributs (ABAC).

Pour obtenir des exemples de politiques basées sur l'identité permettant de limiter l'accès aux tâches des opérations par lot S3 en fonction des balises, consultez Contrôle des autorisations pour les opérations par lot à l'aide de balises de tâche.

ABAC et balises d'objet

Dans les politiques ABAC, les objets utilisent des balises `s3:` plutôt que des balises `aws:`. Pour contrôler l'accès aux objets avec des balises d'objet, vous devez fournir les informations de balise dans l'élément Condition d'une politique avec les balises suivantes :

- `s3:ExistingObjectTag/`*`tag-key`*
- `s3:RequestObjectTagKeys`
- `s3:RequestObjectTag/`*`tag-key`*

Pour plus d'informations sur l'utilisation de balises d'objet pour contrôler l'accès, y compris des exemples de politiques d'autorisation, consultez Stratégies de balisage et de contrôle d'accès.

Utilisation d'informations d'identification temporaires avec Amazon S3

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le

changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. 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.

Transmission des sessions d'accès pour Amazon S3

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

- Le FAS est utilisé par Amazon S3 pour effectuer des appels AWS KMS afin de déchiffrer un objet lorsque SSE-KMS a été utilisé pour le chiffrer. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).
- Les autorisations d'accès S3 utilisent également FAS. Après avoir créé une autorisation d'accès à vos données S3 pour une identité particulière, le bénéficiaire demande un identifiant temporaire aux autorisations d'accès S3. S3 Access Grants obtient un identifiant temporaire pour le demandeur AWS STS et le transmet au demandeur. Pour de plus amples informations, veuillez consulter Demande d'un accès aux données Amazon S3 via les autorisations d'accès S3.

Rôles de service pour Amazon S3

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.

> **Warning**
>
> La modification des autorisations d'un rôle de service peut altérer la fonctionnalité d'Amazon S3. Ne modifiez des rôles de service que quand Amazon S3 vous le conseille.

Rôles liés à un service pour Amazon S3

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 endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Amazon S3 prend en charge les rôles liés au service pour Amazon S3 Storage Lens. Pour plus d'informations sur la création ou la gestion des rôles liés à un service Amazon S3, consultez Utilisation des rôles liés à un service pour Amazon S3 Storage Lens.

Service Amazon S3 en tant que principal

Nom du service dans la politique	Fonctionnalité de S3	En savoir plus
`s3.amazonaws.com`	Réplication S3	Présentation de la configuration de la réplication en direct
`s3.amazonaws.com`	Notifications d'événements S3	Notifications d'événements Amazon S3
`s3.amazonaws.com`	Inventaire S3	Catalogage et analyse de vos données avec l'inventaire S3
`access-grants.s3.amazonaws.com`	Autorisations d'accès S3	Enregistrement d'un emplacement

Nom du service dans la politique	Fonctionnalité de S3	En savoir plus
`batchoperations.s3.amazonaws.com`	Opérations par lot S3	Octroi d'autorisations pour les opérations par lots
`logging.s3.amazonaws.com`	Journalisation des accès au serveur S3	Activation de la journalisation des accès au serveur Amazon S3
`storage-lens.s3.amazonaws.com`	S3 Storage Lens	Afficher les métriques Amazon S3 Storage Lens à l'aide d'une exportation de données

Comment Amazon S3 autorise une demande

Lorsqu'Amazon S3 reçoit une demande : par exemple, une opération de compartiment ou d'objet, il vérifie que le demandeur possède les autorisations nécessaires. Amazon S3 évalue toutes les stratégies d'accès, les politiques utilisateur et les politiques basées sur les ressources (politique de compartiment, liste ACL de compartiment, liste ACL d'objet) pertinentes pour décider d'autoriser ou non la demande.

> **Note**
>
> Si le contrôle des autorisations Amazon S3 ne permet pas de trouver des autorisations valides, une erreur (403 Forbidden) liée à un refus d'accès est renvoyée. Pour plus d'informations, consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3.

Afin de déterminer si le demandeur a l'autorisation d'exécuter l'opération spécifique, Amazon S3 procède comme suit dès réception d'une demande :

1. Convertit toutes les politiques d'accès pertinentes (politique utilisateur, politique de compartiment, etc. ACLs) au moment de l'exécution en un ensemble de politiques à évaluer.
2. Evalue l'ensemble de stratégies obtenu au cours des étapes suivantes. Dans chaque étape, Amazon S3 évalue un sous-ensemble de stratégies dans un contexte spécifique, basé sur l'autorité du contexte.
   a. Contexte d'utilisateur – Dans le contexte d'utilisateur, le compte parent auquel appartient l'utilisateur est l'autorité du contexte.

      Amazon S3 évalue un sous-ensemble de stratégies détenues par le compte parent. Ce sous-ensemble inclut la stratégie d'utilisateur que le parent attache à l'utilisateur. Si le parent possède également la ressource de la demande (compartiment ou objet), Amazon S3 évalue aussi les politiques de ressources correspondantes (politique de compartiment, liste ACL de compartiment et liste ACL d'objet) en même temps.

      Un utilisateur doit avoir l'autorisation du compte parent pour exécuter l'opération.

      Cette étape s'applique uniquement si la demande est faite par un utilisateur dans un Compte AWS. Si la demande est faite à l'aide des informations d'identification de l'utilisateur root d'un Compte AWS, Amazon S3 ignore cette étape.

b. Contexte du compartiment : dans le contexte du compartiment, Amazon S3 évalue les politiques détenues par Compte AWS le propriétaire du compartiment.

   Si la demande concerne une opération de compartiment, le demandeur doit avoir l'autorisation du propriétaire du compartiment. Si la demande concerne un objet, Amazon S3 évalue toutes les stratégies détenues par le propriétaire du compartiment pour vérifier que ce dernier n'a pas refusé explicitement l'accès à l'objet. Si un refus explicite est configuré, Amazon S3 n'autorise pas la demande.

c. Contexte d'objet – Si la demande concerne un objet, Amazon S3 évalue le sous-ensemble de stratégies détenues par le propriétaire de l'objet.

Voici quelques exemples de scénarios qui illustrent comment Amazon S3 autorise une demande.

Example – Le demandeur est un principal IAM

Si le demandeur est un principal IAM, Amazon S3 doit déterminer si le parent auquel Compte AWS appartient le principal a accordé au principal l'autorisation nécessaire pour effectuer l'opération. De plus, si la demande concerne une opération de compartiment, comme une demande pour lister le contenu du compartiment, Amazon S3 doit vérifier que le propriétaire du compartiment a accordé l'autorisation au demandeur d'exécuter l'opération. Pour effectuer une opération spécifique sur une ressource, un principal IAM doit obtenir l'autorisation du parent Compte AWS auquel il appartient et du Compte AWS propriétaire de la ressource.

Example – Le demandeur est un principal IAM : si la demande concerne une opération sur un objet que le propriétaire du compartiment ne possède pas

Si la demande concerne une opération sur un objet que le propriétaire du compartiment ne possède pas, Amazon S3 doit veiller à ce que le demandeur possède l'autorisation du propriétaire de l'objet, mais aussi à ce que la politique de compartiment garantisse que le propriétaire du compartiment n'a pas configuré un refus explicite sur l'objet. Le propriétaire du compartiment (qui paie la facture) peut refuser explicitement l'accès aux objets dans le compartiment, quel que soit le propriétaire. Le propriétaire du compartiment peut également supprimer tout objet du compartiment.

Par défaut, lorsqu'un autre Compte AWS utilisateur télécharge un objet dans votre compartiment à usage général S3, ce compte (le rédacteur de l'objet) est propriétaire de l'objet, y a accès et peut autoriser d'autres utilisateurs à y accéder via des listes de contrôle d'accès (ACLs). Vous pouvez utiliser Object Ownership pour modifier ce comportement par défaut afin qu'il soit ACLs désactivé et que vous, en tant que propriétaire du bucket, soyez automatiquement propriétaire de tous les objets

de votre bucket à usage général. Par conséquent, le contrôle d'accès à vos données est basé sur des politiques, telles que les politiques utilisateur IAM, les politiques relatives aux compartiments S3, les politiques relatives aux points de terminaison du cloud privé virtuel (VPC) AWS Organizations et les politiques de contrôle des services (). SCPs Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Pour en savoir plus sur la façon dont Amazon S3 évalue les stratégies d'accès pour autoriser ou refuser les demandes d'opérations de compartiment et d'objets, consultez les rubriques suivantes :

Rubriques

- Comment Amazon S3 autorise une demande pour une opération de compartiment
- Comment Amazon S3 autorise une demande pour une opération sur les objets

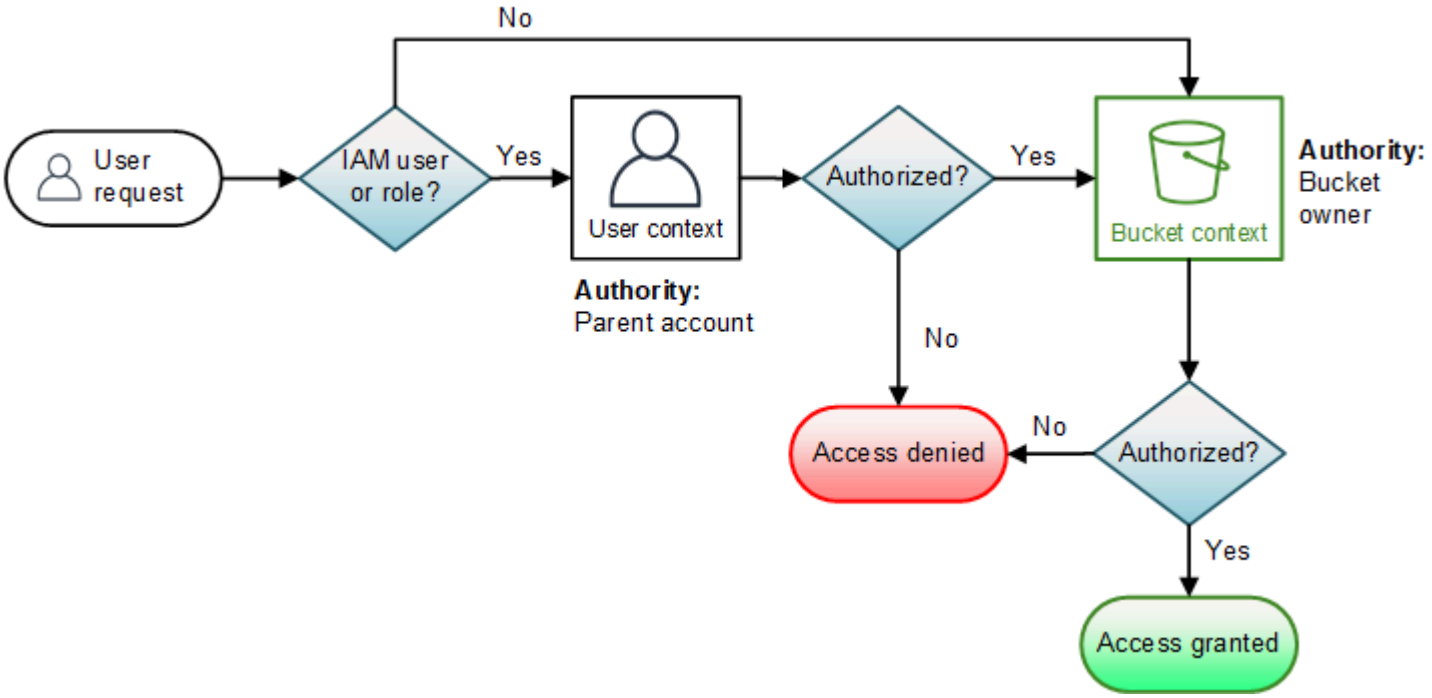
Comment Amazon S3 autorise une demande pour une opération de compartiment

Lorsqu'Amazon S3 reçoit une demande d'opération de compartiment, Amazon S3 convertit toutes les autorisations pertinentes en un ensemble de stratégies à évaluer lors de l'exécution. Les autorisations pertinentes incluent les autorisations basées sur les ressources (par exemple, les stratégies de compartiment et les listes de contrôle d'accès des compartiments) et les stratégies utilisateur si la demande provient d'un principal IAM. Amazon S3 évalue ensuite l'ensemble de politiques obtenu au cours d'une série d'étapes conformément à un contexte spécifique : contexte de l'utilisateur ou du compartiment.

1. Contexte utilisateur — Si le demandeur est un principal IAM, le principal doit avoir l'autorisation du parent Compte AWS auquel il appartient. Dans cette étape, Amazon S3 évalue un sous-ensemble de stratégies détenues par le compte parent (également appelé autorité du contexte). Ce sous-ensemble de stratégies inclut la stratégie d'utilisateur que le compte parent attache au principal. Si le parent détient également la ressource de la demande (dans ce cas, le compartiment), Amazon S3 évalue également les stratégies de ressources correspondantes (politique de compartiment et liste ACL de compartiment) en même temps. Lorsqu'une demande pour une opération de compartiment est faite, les journaux d'accès au serveur enregistre l'ID canonique du demandeur. Pour plus d'informations, consultez Enregistrement de demandes avec journalisation des accès au serveur.
2. Contexte de compartiment – Le demandeur doit avoir l'autorisation du propriétaire du compartiment pour exécuter une opération de compartiment spécifique. Au cours de cette étape, Amazon S3 évalue un sous-ensemble de politiques appartenant au propriétaire du Compte AWS compartiment.

Le propriétaire du compartiment peut accorder l'autorisation grâce à la politique de compartiment ou la liste ACL de compartiment. Si le Compte AWS qui détient le compartiment est également le compte parent d'un principal IAM, il peut configurer les autorisations du compartiment dans une politique utilisateur.

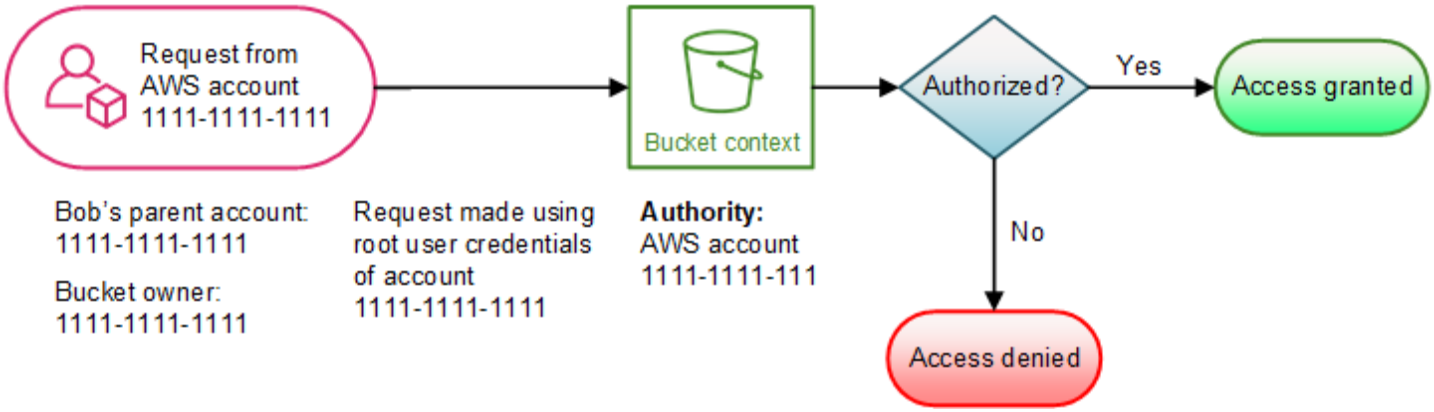
Voici un schéma de l'évaluation basée sur le contexte pour les opérations de compartiment.



Les exemples suivants illustrent la logique d'évaluation.

Exemple 1 : Opération de compartiment demandée par le propriétaire du compartiment

Dans cet exemple, le propriétaire du compartiment envoie une demande pour une opération de compartiment grâce aux informations d'identification racine du Compte AWS.

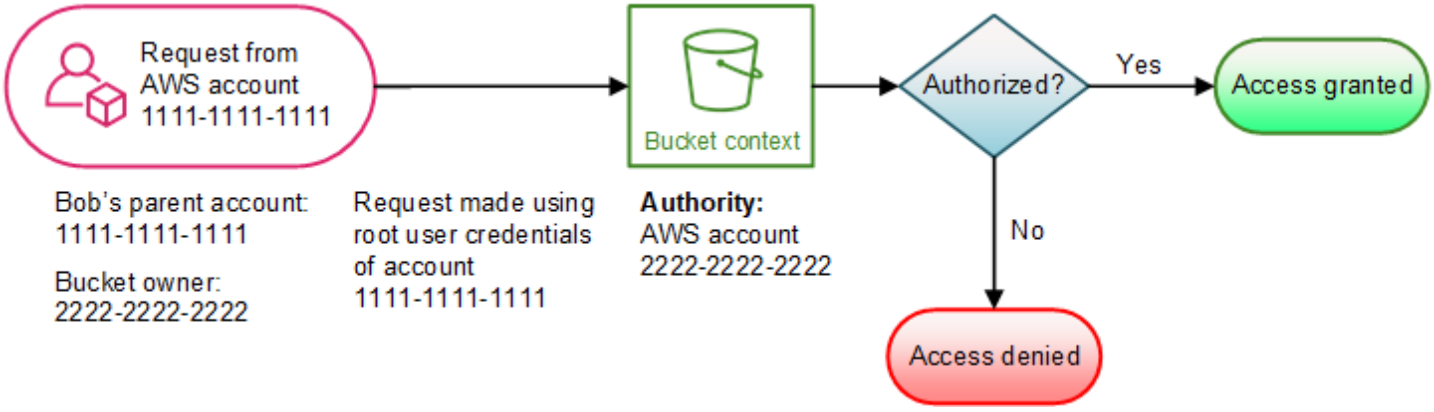


Amazon S3 réalise l'évaluation du contexte comme suit :

1. Étant donné que la demande a été faite grâce aux informations d'identification d'utilisateur root d'un Compte AWS, le contexte d'utilisateur n'est pas évalué.
2. Dans le contexte de compartiment, Amazon S3 examine la politique de compartiment pour déterminer si le demandeur a l'autorisation d'exécuter l'opération. Amazon S3 autorise la demande.

Exemple 2 : opération de compartiment demandée par une personne Compte AWS qui n'est pas le propriétaire du compartiment

Dans cet exemple, une demande est faite grâce aux informations d'identification d'utilisateur root du Compte AWS 1111-1111-1111 pour une opération de compartiment détenue par le Compte AWS 2222-2222-2222. Aucun utilisateur IAM n'est impliqué dans cette demande.

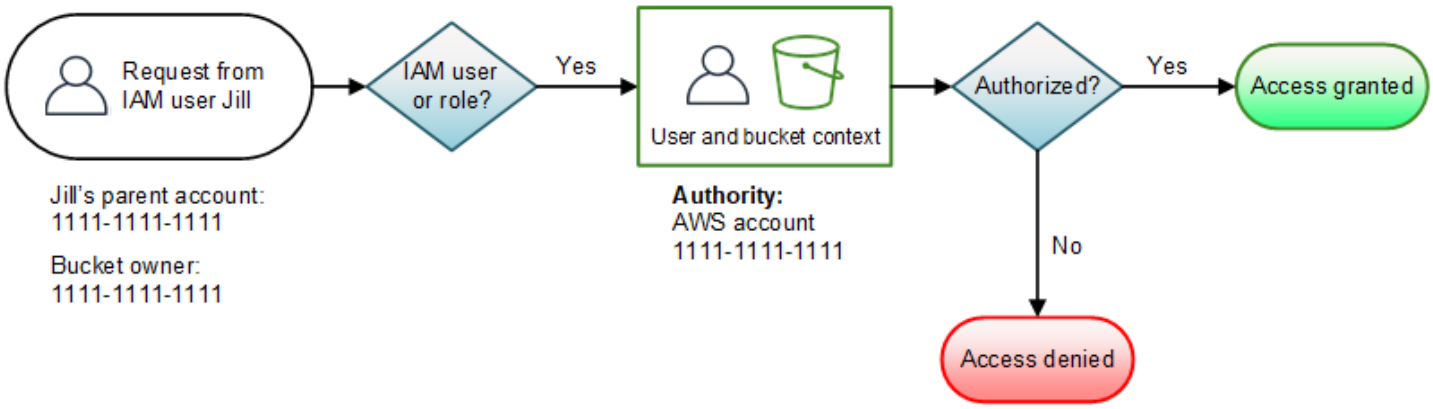


Dans cet exemple, Amazon S3 évalue le contexte comme suit :

1. Comme la demande est faite à l'aide des informations d'identification de l'utilisateur root d'un Compte AWS, le contexte utilisateur n'est pas évalué.
2. Dans le contexte de compartiment, Amazon S3 examine la politique de compartiment. Si le propriétaire du compartiment (Compte AWS 2222-2222-2222) n'a pas autorisé le Compte AWS 1111-1111-1111 à effectuer l'opération demandée, Amazon S3 refuse la demande. Sinon, Amazon S3 accorde la demande et exécute l'opération.

Exemple 3 : opération de compartiment demandée par un directeur IAM dont le parent Compte AWS est également le propriétaire du compartiment

Dans l'exemple, la demande est envoyée par Jill, une utilisatrice IAM du Compte AWS 1111-1111-1111, qui détient également le compartiment.



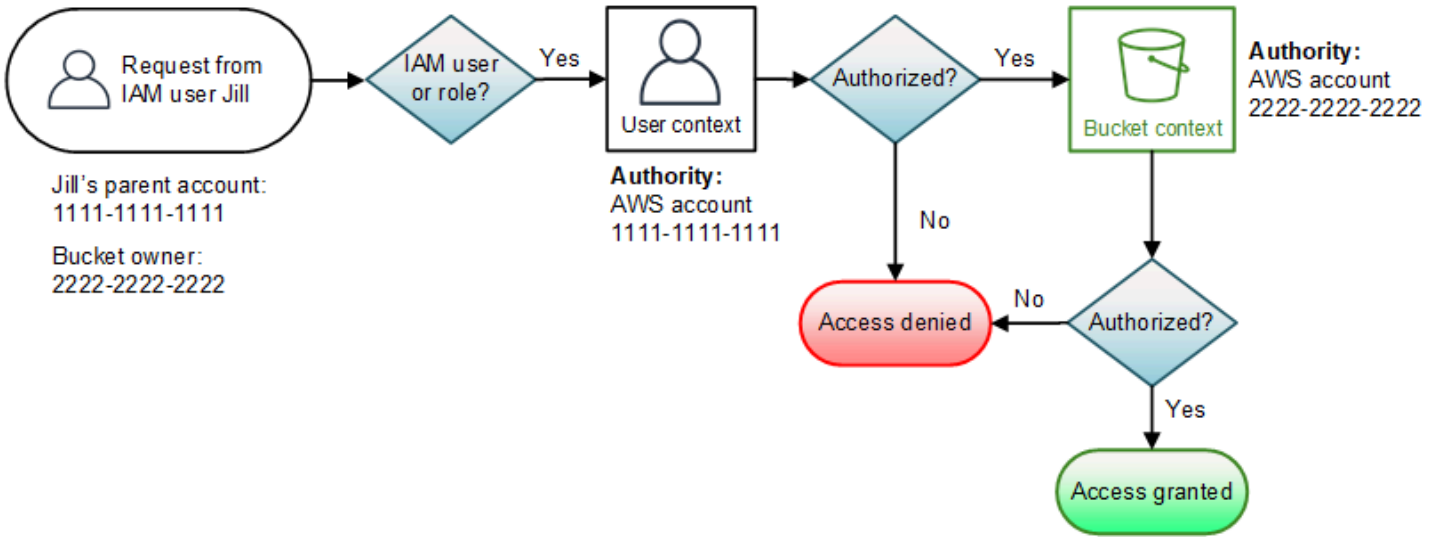
Amazon S3 réalise l'évaluation suivante du contexte :

1. Comme la demande provient d'un principal IAM, dans le contexte de l'utilisateur, Amazon S3 évalue toutes les politiques appartenant au parent Compte AWS afin de déterminer si Jill est autorisée à effectuer l'opération.

   Dans cet exemple, le parent Compte AWS 1111-1111-1111, auquel appartient le principal, est également le propriétaire du compartiment. Ainsi, outre la politique utilisateur, Amazon S3 évalue également la politique de compartiment et la liste ACL de compartiment dans le même contexte, car elles appartiennent au même compte.
2. Amazon S3 a évalué la politique de compartiment et la liste ACL de compartiment dans le contexte d'utilisateur, il n'a dont pas évalué le contexte de compartiment.

Exemple 4 : opération de compartiment demandée par un principal IAM dont le parent n' Compte AWS est pas le propriétaire du compartiment

Dans cet exemple, la demande est envoyée par Jill, une utilisatrice IAM dont le parent Compte AWS est 1111-1111-1111, mais le bucket appartient à un autre utilisateur, 2222-2222-2222. Compte AWS



Jill aura besoin des autorisations du parent Compte AWS et du propriétaire du compartiment. Amazon S3 évalue le contexte comme suit :

1. Étant donné que la demande provient d'un principal IAM, Amazon S3 évalue le contexte d'utilisateur en examinant les stratégies autorisées par le compte pour vérifier que Jill possède les autorisations nécessaires. Si Jill a l'autorisation, Amazon S3 passe à l'évaluation du contexte du compartiment. Si Jill n'a pas l'autorisation, la demande est refusée.
2. Dans le contexte du compartiment, Amazon S3 vérifie que le propriétaire du compartiment 2222-2222-2222 a accordé à Jill (ou à ses parents Compte AWS) l'autorisation d'effectuer l'opération demandée. Si elle a cette autorisation, Amazon S3 autorise la demande et exécute l'opération. Sinon, Amazon S3 refuse la demande.

Comment Amazon S3 autorise une demande pour une opération sur les objets

Lorsqu'Amazon S3 reçoit une demande pour une opération d'objet, il convertit toutes les autorisations pertinentes, comme les autorisations basées sur les ressources (liste de contrôle d'accès d'objet, politique de compartiment, liste de contrôle d'accès (ACL) de compartiment) et les stratégies d'utilisateur IAM, en un ensemble de stratégies à évaluer au moment de l'exécution. Ensuite, il évalue l'ensemble de stratégies obtenu au cours d'une série d'étapes. Dans chaque étape, il évalue un sous-ensemble de politiques dans trois contextes spécifiques : contexte de l'utilisateur, du compartiment et de l'objet.

1. Contexte utilisateur — Si le demandeur est un principal IAM, le principal doit avoir l'autorisation du parent Compte AWS auquel il appartient. Dans cette étape, Amazon S3 évalue un sous-ensemble de stratégies détenues par le compte parent (également appelé autorité du contexte). Ce sous-

ensemble de stratégies inclut la stratégie d'utilisateur que le parent attache au principal. Si le parent possède également la ressource de la demande (compartiment ou objet), Amazon S3 évalue les politiques de ressources correspondantes (politique de compartiment, liste ACL de compartiment et liste ACL d'objet) en même temps.

> **Note**
>
> Si le parent Compte AWS est propriétaire de la ressource (bucket ou objet), il peut accorder des autorisations de ressource à son principal IAM en utilisant la politique utilisateur ou la politique de ressource.

2. Contexte de compartiment – Dans ce contexte, Amazon S3 évalue les stratégies détenues par le Compte AWS propriétaire du compartiment.

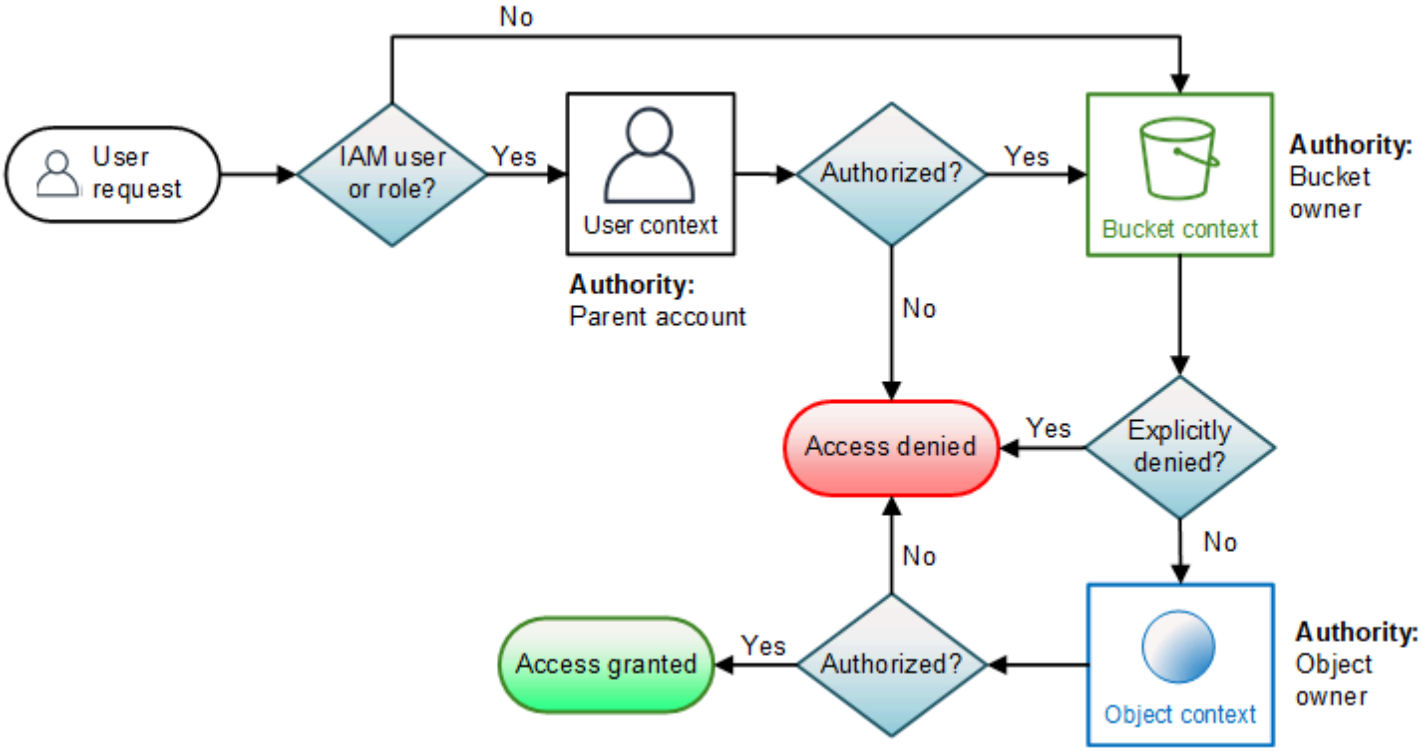
   Si le Compte AWS propriétaire de l'objet indiqué dans la demande n'est pas le même que le propriétaire du compartiment, Amazon S3 vérifie les politiques si le propriétaire du compartiment a explicitement refusé l'accès à l'objet. Si un refus explicite est configuré sur l'objet, Amazon S3 n'autorise pas la demande.

3. Contexte d'objet – Le demandeur doit avoir l'autorisation du propriétaire de l'objet pour exécuter une opération d'objet spécifique. Dans cette étape, Amazon S3 évalue la liste ACL d'objet.

   > **Note**
   >
   > Si les propriétaires du compartiment et de l'objet sont les mêmes, l'accès à l'objet peut être autorisé dans la politique de compartiment, qui est évaluée dans le contexte de compartiment. Si les propriétaires sont différents, les propriétaires de l'objet doivent utiliser une liste ACL d'objet pour accorder les autorisations. Si le Compte AWS propriétaire de l'objet est également le compte parent auquel appartient le principal IAM, celui-ci peut configurer les autorisations de l'objet dans une politique utilisateur, qui est évaluée dans le contexte de l'utilisateur. Pour en savoir plus sur l'utilisation de ces alternatives de stratégie d'accès, consultez Procédures détaillées qui utilisent des politiques pour gérer l'accès à vos ressources Amazon S3.
   > Si, en tant que propriétaire du compartiment, vous souhaitez posséder tous les objets de votre compartiment et utiliser des politiques de compartiment ou des politiques basées sur la IAMto gestion de l'accès à ces objets, vous pouvez appliquer le paramètre imposé par le propriétaire du compartiment pour la propriété des objets. Avec ce paramètre, en tant que propriétaire du compartiment, vous possédez automatiquement tous les objets de votre

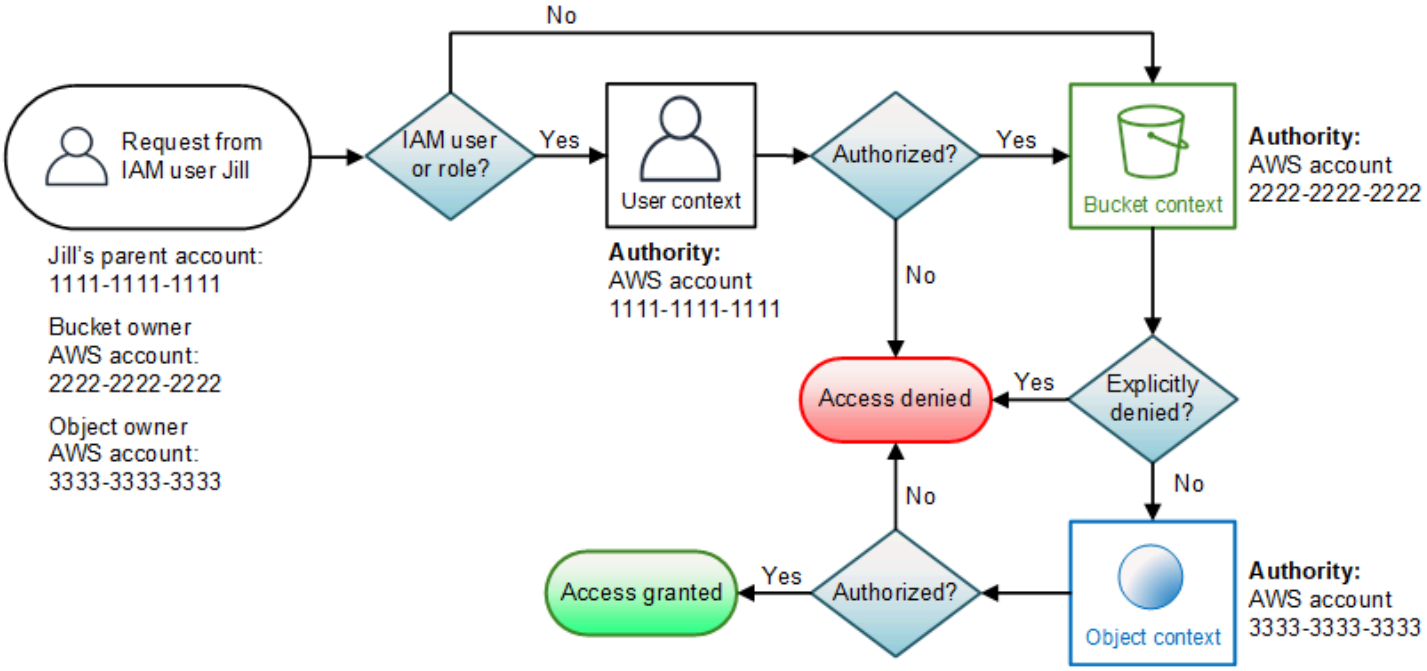
compartiment et avez le contrôle total sur chaque objet présents dans votre compartiment. Le bucket et l'objet ne ACLs peuvent pas être modifiés et leur accès n'est plus pris en compte. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Voici un schéma de l'évaluation basée sur le contexte pour les opérations d'objet.



Exemple de demande d'opération d'objet

Dans cet exemple, l'utilisateur IAM Jill, dont le parent Compte AWS est 1111-1111-1111, envoie une demande d'opération d'objet (par exemple,`GetObject`) pour un objet appartenant à Compte AWS 3333-3333-3333 dans un bucket appartenant au 2222-2222-2222. Compte AWS



Jill aura besoin de l'autorisation du parent Compte AWS, du propriétaire du bucket et du propriétaire de l'objet. Amazon S3 évalue le contexte comme suit :

1. Comme la demande provient d'un principal IAM, Amazon S3 évalue le contexte utilisateur pour vérifier que le parent Compte AWS 1111-1111-1111 a autorisé Jill à effectuer l'opération demandée. Si Jill a l'autorisation, Amazon S3 évalue le contexte de compartiment. Sinon, Amazon S3 refuse la demande.
2. Dans le contexte du bucket, le propriétaire du bucket, Compte AWS 2222-2222-2222, est l'autorité du contexte. Amazon S3 évalue la politique de compartiment pour déterminer si le propriétaire du compartiment a explicitement refusé que Jill accède à l'objet.
3. Dans le contexte de l'objet, l'autorité du contexte est le Compte AWS 3333-3333-3333, le propriétaire de l'objet. Amazon S3 évalue la liste ACL d'objet pour déterminer si Jill a l'autorisation d'accéder à l'objet. Si oui, Amazon S3 autorise la demande.

Autorisations requises pour les opérations d'API Amazon S3

> **Note**
>
> Cette page traite des actions de politique Amazon S3 pour les compartiments à usage général. Pour en savoir plus sur les actions de politique Amazon S3 pour les compartiments de répertoires, consultez Actions spécifiques aux compartiments de répertoires.

Pour effectuer une opération d'API S3, vous devez disposer des autorisations appropriées. Cette page associe les opérations d'API S3 aux autorisations requises. Pour accorder des autorisations permettant d'effectuer une opération d'API S3, vous devez élaborer une politique valide (telle qu'une politique de compartiment S3 ou une politique basée sur l'identité IAM) et spécifier les actions correspondantes dans l'élément `Action` de cette politique. Ces actions sont appelées actions de politique. Toutes les opérations d'API S3 ne sont pas représentées par une autorisation unique (une seule action de politique), et certaines autorisations (certaines actions de politique) sont obligatoires pour de nombreuses opérations d'API différentes.

Lorsque vous créez des politiques, vous devez spécifier l'élément `Resource` en fonction du type de ressource approprié requis par les actions de politique Amazon S3 correspondantes. Cette page classe les autorisations relatives aux opérations d'API S3 par type de ressource. Pour de plus d'informations sur les types de ressources, consultez Types de ressources définis par Amazon S3 dans la Référence de l'autorisation de service. Pour obtenir une liste complète des actions de politique, des clés de condition et des ressources Amazon S3 que vous pouvez utiliser dans les politiques, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service. Pour obtenir la liste des opérations d'API Amazon S3, consultez Actions d'API Amazon S3 dans la Référence d'API Amazon Simple Storage Service.

Pour plus d'informations sur la manière de traiter les `403 Forbidden` erreurs HTTP dans S3, consultezRésolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3. Pour plus d'informations sur les fonctionnalités IAM à utiliser avec S3, consultezFonctionnement d'Amazon S3 avec IAM. Pour plus d'informations sur les meilleures pratiques de sécurité S3, consultezBonnes pratiques de sécurité pour Amazon S3.

Rubriques

- Opérations de compartiment et autorisations
- Opérations d'objet et autorisations

- Point d'accès pour les opérations et autorisations de buckets à usage général
- Opérations de point d'accès Object Lambda et autorisations
- Opérations de point d'accès multi-régions et autorisations
- Opérations relatives aux tâches par lots et autorisations
- Opérations de configuration S3 Storage Lens et autorisations
- Opérations des groupes S3 Storage Lens et autorisations
- Opérations et autorisations de l'instance S3 Access Grants
- S3 Access accorde des autorisations et des opérations de localisation
- Les subventions d'accès S3 octroient des opérations et des autorisations
- Opérations de compte et autorisations

Opérations de compartiment et autorisations

Les opérations de compartiment sont des opérations d'API S3 qui opèrent sur le type de ressource du compartiment. Vous devez spécifier les actions de politique S3 pour les opérations de compartiment dans les politiques de compartiment ou les politiques basées sur l'identité IAM.

Dans les politiques, l'élément `Resource` doit correspondre à l'Amazon Resource Name (ARN) du compartiment. Pour obtenir plus d'informations sur le format des éléments `Resource` et pour voir des exemples de politiques, consultez Opérations de compartiment.

> **Note**
>
> Pour accorder des autorisations aux opérations de compartiment dans les stratégies de point d'accès, notez ce qui suit :
>
> - Les autorisations accordées pour les opérations de compartiment dans une stratégie de point d'accès ne sont effectives que si le compartiment sous-jacent accorde également les mêmes autorisations. Lorsque vous utilisez un point d'accès, vous devez déléguer le contrôle d'accès du compartiment à ce point d'accès ou ajouter les autorisations de la politique du point d'accès à la politique du compartiment sous-jacent.
> - Dans les stratégies de point d'accès qui accordent des autorisations pour les opérations de compartiment, l'élément `Resource` doit être l'ARN d'`accesspoint`. Pour obtenir plus d'informations sur le format des éléments `Resource` et pour voir des exemples de politiques, consultez Opérations relatives aux compartiments dans les politiques relatives aux points d'accès pour les compartiments à usage général. Pour plus d'informations

sur les stratégies des points d'accès, consultez Configuration des politiques IAM pour l'utilisation des points d'accès.

- Les opérations de compartiment ne sont pas toutes prises en charge par les points d'accès. Pour de plus amples informations, veuillez consulter Compatibilité des points d'accès avec les opérations S3.

Vous trouverez ci-dessous le mappage des opérations de compartiment et des actions de politiques requises.

Opérations d'API	Actions de politique	Description des actions de politique
CreateBucket	(Obligatoire) `s3:CreateBucket`	Obligatoire pour créer un compartiment S3.
	(Obligatoire sous condition) `s3:PutBucketAcl`	Obligatoire si vous souhaitez utiliser une liste de contrôle d'accès (ACL) pour spécifier des autorisations sur un compartiment lorsque vous effectuez une demande `CreateBucket` .
	(Obligatoire sous condition) `s3:PutBucketObjectLockConfiguration` , `s3:PutBucketVersioning`	Obligatoire si vous souhaitez activer le verrouillage d'objet lors de la création d'un compartiment.
	(Obligatoire sous condition) `s3:PutBucketOwnershipControls`	Obligatoire si vous souhaitez spécifier la propriété d'objets S3 lors de la création d'un compartiment.
CreateBucketMetadataConfiguration(Fonctionnement de l'API V2). Le nom de l'action	(Obligatoire) `s3:CreateBucketMet`	Obligatoire pour créer une configuration de table de métadonnées sur un

Opérations d'API	Actions de politique	Description des actions de politique
de politique IAM est le même pour les opérations d'API V1 et V2.)	`adataTableConfigur ation s3tables: CreateTab leBucket ,s3tables: CreateNam espace ,s3tables: CreateTable ,s3tables: GetTable ,s3tables: PutTableP olicy ,s3tables: PutTableEncryption , kms:DescribeKey`	compartiment à usage général. Pour créer votre compartim ent de tables AWS géré et les tables de métadonnées spécifiées dans la configura tion de votre table de métadonnées, vous devez disposer des `s3tables` autorisations spécifiées. Si vous souhaitez chiffrer vos tables de métadonnées à l'aide du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), vous devez disposer d'autorisations supplémentaires dans votre politique de clés KMS. Pour de plus amples informations, veuillez consulter the section called "Autorisations pour les tables de métadonnées". Si vous souhaitez également intégrer votre compartim ent de tables AWS géré aux services AWS d'analyse afin de pouvoir interroger votre table de métadonnées, vous avez besoin d'autorisations supplémentaires. Pour plus d'informations, consultez

Opérations d'API	Actions de politique	Description des actions de politique
		Intégration des tables Amazon S3 aux services d'analytique AWS.

Opérations d'API	Actions de politique	Description des actions de politique
CreateBucketMetadataTableConfiguration(fonctionnement de l'API V1)	(Obligatoire) `s3:CreateBucketMetadataTableConfiguration` , `s3tables:CreateNamespace` , `s3tables:CreateTable` , `s3tables:GetTable` , `s3tables:PutTablePolicy`	Obligatoire pour créer une configuration de table de métadonnées sur un compartiment à usage général. Pour créer la table de métadonnées dans le compartiment de tables indiqué dans la configuration de votre table de métadonnées, vous devez disposer des autorisations `s3tables` spécifiées. Si vous souhaitez chiffrer vos tables de métadonnées à l'aide d'un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), vous avez besoin d'autorisations supplémentaires. Pour de plus amples informations, veuillez consulter the section called "Autorisations pour les tables de métadonnées". Si vous souhaitez également intégrer votre compartiment de tables aux services AWS d'analyse afin de pouvoir interroger votre table de métadonnées, vous

Opérations d'API	Actions de politique	Description des actions de politique
		avez besoin d'autorisations supplémentaires. Pour plus d'informations, consultez Intégration des tables Amazon S3 aux services AWS d'analyse.
DeleteBucket	(Obligatoire) `s3:DeleteBucket`	Obligatoire pour supprimer un compartiment S3.
DeleteBucketAnalyticsConfiguration	(Obligatoire) `s3:PutAnalyticsConfiguration`	Obligatoire pour supprimer une configuration d'analytique S3 d'un compartiment S3.
DeleteBucketCors	(Obligatoire) `s3:PutBucketCORS`	Obligatoire pour supprimer la configuration du partage des ressources cross-origin (CORS) pour un compartiment.
DeleteBucketEncryption	(Obligatoire) `s3:PutEncryptionConfiguration`	Obligatoire pour réinitialiser la configuration du chiffrement par défaut d'un compartiment S3 en tant que chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).
DeleteBucketIntelligentTieringConfiguration	(Obligatoire) `s3:PutIntelligentTieringConfiguration`	Obligatoire pour supprimer la configuration S3 Intelligent-Tiering existante d'un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
DeleteBucketInventoryConfiguration	(Obligatoire) `s3:PutInventoryConfiguration`	Obligatoire pour supprimer une configuration d'inventaire S3 d'un compartiment S3.
DeleteBucketLifecycle	(Obligatoire) `s3:PutLifecycleConfiguration`	Obligatoire pour supprimer la configuration de cycle de vie S3 pour un compartiment S3.
DeleteBucketMetadataConfiguration(Fonctionnement de l'API V2). Le nom de l'action de politique IAM est le même pour les opérations d'API V1 et V2.)	(Obligatoire) `s3:DeleteBucketMetadataTableConfiguration`	Obligatoire pour supprimer une configuration de table de métadonnées d'un compartiment à usage général.
DeleteBucketMetadataTableConfiguration(fonctionnement de l'API V1)	(Obligatoire) `s3:DeleteBucketMetadataTableConfiguration`	Obligatoire pour supprimer une configuration de table de métadonnées d'un compartiment à usage général.
DeleteBucketMetricsConfiguration	(Obligatoire) `s3:PutMetricsConfiguration`	Nécessaire pour supprimer une configuration de métriques pour les métriques de CloudWatch demande Amazon d'un compartiment S3.
DeleteBucketOwnershipControls	(Obligatoire) `s3:PutBucketOwnershipControls`	Obligatoire pour supprimer le paramètre Propriété d'objets pour un compartiment S3. Après la suppression, le paramètre Propriété d'objets devient `Object writer`.

Opérations d'API	Actions de politique	Description des actions de politique
DeleteBucketPolicy	(Obligatoire) `s3:DeleteBucketPolicy`	Obligatoire pour supprimer la politique d'un compartiment S3.
DeleteBucketReplication	(Obligatoire) `s3:PutReplicationConfiguration`	Obligatoire pour supprimer la configuration de réplication d'un compartiment S3.
DeleteBucketTagging	(Obligatoire) `s3:PutBucketTagging`	Obligatoire pour supprimer des balises d'un compartiment S3.
DeleteBucketWebsite	(Obligatoire) `s3:DeleteBucketWebsite`	Obligatoire pour supprimer la configuration de site web pour un compartiment S3.
DeletePublicAccessBlock (au niveau du compartiment)	(Obligatoire) `s3:PutBucketPublicAccessBlock`	Obligatoire pour supprimer la configuration du blocage de l'accès public pour un compartiment S3.
GetBucketAccelerateConfiguration	(Obligatoire) `s3:GetAccelerateConfiguration`	Obligatoire pour utiliser la sous-ressource d'accélération afin de renvoyer l'état Amazon S3 Transfer Acceleration (Activé ou Suspendu) d'un compartiment.
GetBucketAcl	(Obligatoire) `s3:GetBucketAcl`	Obligatoire pour renvoyer la liste de contrôle d'accès (ACL) d'un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
GetBucketAnalyticsConfiguration	(Obligatoire) `s3:GetAnalyticsConfiguration`	Obligatoire pour renvoyer une configuration d'analytique identifiée par l'ID de configuration d'analytique à partir d'un compartiment S3.
GetBucketCors	(Obligatoire) `s3:GetBucketCORS`	Obligatoire pour renvoyer la configuration du partage des ressources cross-origin (CORS) pour un compartiment S3.
GetBucketEncryption	(Obligatoire) `s3:GetEncryptionConfiguration`	Obligatoire pour renvoyer la configuration du chiffrement par défaut pour un compartiment S3.
GetBucketIntelligentTieringConfiguration	(Obligatoire) `s3:GetIntelligentTieringConfiguration`	Obligatoire pour obtenir la configuration S3 Intelligent-Tiering d'un compartiment S3.
GetBucketInventoryConfiguration	(Obligatoire) `s3:GetInventoryConfiguration`	Obligatoire pour renvoyer une configuration d'inventaire identifiée par l'ID de configuration d'inventaire à partir du compartiment.
GetBucketLifecycle	(Obligatoire) `s3:GetLifecycleConfiguration`	Obligatoire pour renvoyer la configuration de cycle de vie S3 du compartiment.
GetBucketLocation	(Obligatoire) `s3:GetBucketLocation`	Nécessaire pour renvoyer Région AWS le compartiment dans lequel réside un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
GetBucketLogging	(Obligatoire) `s3:GetBucketLogging`	Obligatoire pour renvoyer le statut de journalisation d'un compartiment S3 et les autorisations dont disposent les utilisateurs pour afficher et modifier ce statut.
GetBucketMetadataConfiguration(Fonctionnement de l'API V2). Le nom de l'action de politique IAM est le même pour les opérations d'API V1 et V2.)	(Obligatoire) `s3:GetBucketMetadataTableConfiguration`	Obligatoire pour récupérer une configuration de table de métadonnées pour un compartiment à usage général.
GetBucketMetadataTableConfiguration(fonctionnement de l'API V1)	(Obligatoire) `s3:GetBucketMetadataTableConfiguration`	Obligatoire pour récupérer une configuration de table de métadonnées pour un compartiment à usage général.
GetBucketMetricsConfiguration	(Obligatoire) `s3:GetMetricsConfiguration`	Obligatoire pour obtenir une configuration de métriques spécifiée par l'ID de configuration de métriques à partir du compartiment.
GetBucketNotificationConfiguration	(Obligatoire) `s3:GetBucketNotification`	Obligatoire pour renvoyer la configuration de notification d'un compartiment S3.
GetBucketOwnershipControls	(Obligatoire) `s3:GetBucketOwnershipControls`	Obligatoire pour récupérer le paramètre Propriété d'objets pour un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
GetBucketPolicy	(Obligatoire) `s3:GetBucketPolicy`	Obligatoire pour renvoyer la politique d'un compartiment S3.
GetBucketPolicyStatus	(Obligatoire) `s3:GetBucketPolicyStatus`	Obligatoire pour récupérer le statut de la politique d'un compartiment S3, indiquant si ce compartiment est public.
GetBucketReplication	(Obligatoire) `s3:GetReplicationConfiguration`	Obligatoire pour renvoyer la configuration de réplication d'un compartiment S3.
GetBucketRequestPayment	(Obligatoire) `s3:GetBucketRequestPayment`	Obligatoire pour renvoyer la configuration du paiement des demandes pour un compartiment S3.
GetBucketVersioning	(Obligatoire) `s3:GetBucketVersioning`	Obligatoire pour renvoyer l'état de la gestion des versions d'un compartiment S3.
GetBucketTagging	(Obligatoire) `s3:GetBucketTagging`	Obligatoire pour renvoyer l'ensemble de balises associé à un compartiment S3.
GetBucketWebsite	(Obligatoire) `s3:GetBucketWebsite`	Obligatoire pour renvoyer la configuration de site web pour un compartiment S3.
GetObjectLockConfiguration	(Obligatoire) `s3:GetBucketObjectLockConfiguration`	Obligatoire pour obtenir la configuration du verrouillage d'objet pour un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
GetPublicAccessBlock (au niveau du compartiment)	(Obligatoire) `s3:GetBucketPublicAccessBlock`	Obligatoire pour récupérer la configuration du blocage de l'accès public pour un compartiment S3.
HeadBucket	(Obligatoire) `s3:ListBucket`	Obligatoire pour déterminer s'il existe un compartiment et si vous avez l'autorisation d'y accéder.
ListBucketAnalyticsConfigurations	(Obligatoire) `s3:GetAnalyticsConfiguration`	Obligatoire pour répertorier les configurations d'analytique pour un compartiment S3.
ListBucketIntelligentTieringConfigurations	(Obligatoire) `s3:GetIntelligentTieringConfiguration`	Obligatoire pour répertorier les configurations S3 Intelligent-Tiering d'un compartiment S3.
ListBucketInventoryConfigurations	(Obligatoire) `s3:GetInventoryConfiguration`	Obligatoire pour renvoyer une liste des configurations d'inventaire pour un compartiment S3.
ListBucketMetricsConfigurations	(Obligatoire) `s3:GetMetricsConfiguration`	Obligatoire pour répertorier les configurations de métriques pour un compartiment S3.
ListObjects	(Obligatoire) `s3:ListBucket`	Obligatoire pour répertorier une partie ou la totalité des objets (jusqu'à 1 000 objets) d'un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `s3:GetObjectAcl`	Obligatoire si vous souhaitez afficher les informations relatives au propriétaire de l'objet.
ListObjectsV2	(Obligatoire) `s3:ListBucket`	Obligatoire pour répertorier une partie ou la totalité des objets (jusqu'à 1 000 objets) d'un compartiment S3.
	(Obligatoire sous condition) `s3:GetObjectAcl`	Obligatoire si vous souhaitez afficher les informations relatives au propriétaire de l'objet.
ListObjectVersions	(Obligatoire) `s3:ListBucketVersions`	Obligatoire pour obtenir les métadonnées relatives à toutes les versions des objets d'un compartiment S3.
PutBucketAccelerateConfiguration	(Obligatoire) `s3:PutAccelerateConfiguration`	Obligatoire pour définir la configuration accélérée d'un compartiment existant.
PutBucketAcl	(Obligatoire) `s3:PutBucketAcl`	Nécessaire pour utiliser des listes de contrôle d'accès (ACLs) pour définir les autorisations sur un bucket existant.
PutBucketAnalyticsConfiguration	(Obligatoire) `s3:PutAnalyticsConfiguration`	Obligatoire pour définir une configuration d'analytique pour un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
PutBucketCors	(Obligatoire) `s3:PutBucketCORS`	Obligatoire pour définir la configuration du partage des ressources cross-origin (CORS) pour un compartiment S3.
PutBucketEncryption	(Obligatoire) `s3:PutEncryptionConfiguration`	Obligatoire pour configurer le chiffrement par défaut pour un compartiment S3.
PutBucketIntelligentTieringConfiguration	(Obligatoire) `s3:PutIntelligentTieringConfiguration`	Obligatoire pour attribuer la configuration S3 Intelligent-Tiering à un compartiment S3.
PutBucketInventoryConfiguration	(Obligatoire) `s3:PutInventoryConfiguration`	Obligatoire pour ajouter une configuration d'inventaire à un compartiment S3.
PutBucketLifecycle	(Obligatoire) `s3:PutLifecycleConfiguration`	Obligatoire pour créer une configuration de cycle de vie S3 ou pour remplacer une configuration de cycle de vie existante pour un compartiment S3.
PutBucketLogging	(Obligatoire) `s3:PutBucketLogging`	Obligatoire pour définir les paramètres de journalisation d'un compartiment S3 et pour spécifier les autorisations définissant qui peut consulter et modifier ces paramètres.

Opérations d'API	Actions de politique	Description des actions de politique
PutBucketMetricsConfiguration	(Obligatoire) `s3:PutMetricsConfiguration`	Nécessaire pour définir ou mettre à jour une configuration de métriques pour les métriques de CloudWatch demande Amazon d'un compartiment S3.
PutBucketNotificationConfiguration	(Obligatoire) `s3:PutBucketNotification`	Obligatoire pour activer les notifications d'événements spécifiés pour un compartiment S3.
PutBucketOwnershipControls	(Obligatoire) `s3:PutBucketOwnershipControls`	Obligatoire pour créer ou modifier le paramètre Propriété d'objets pour un compartiment S3.
PutBucketPolicy	(Obligatoire) `s3:PutBucketPolicy`	Obligatoire pour appliquer une politique de compartiment S3 à un compartiment.
PutBucketReplication	(Obligatoire) `s3:PutReplicationConfiguration`	Obligatoire pour créer une configuration de réplication ou pour remplacer une configuration existante pour un compartiment S3.
PutBucketRequestPayment	(Obligatoire) `s3:PutBucketRequestPayment`	Obligatoire pour définir la configuration du paiement des demandes pour un compartiment.
PutBucketTagging	(Obligatoire) `s3:PutBucketTagging`	Obligatoire pour ajouter un ensemble de balises à un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
PutBucketVersioning	(Obligatoire) `s3:PutBucketVersioning`	Obligatoire pour définir l'état de la gestion des versions d'un compartiment S3.
PutBucketWebsite	(Obligatoire) `s3:PutBucketWebsite`	Obligatoire pour configurer un compartiment en tant que site web et pour définir la configuration de ce site web.
PutObjectLockConfiguration	(Obligatoire) `s3:PutBucketObjectLockConfiguration`	Obligatoire pour appliquer la configuration du verrouillage d'objet à un compartiment S3.
PutPublicAccessBlock (au niveau du compartiment)	(Obligatoire) `s3:PutBucketPublicAccessBlock`	Obligatoire pour créer ou modifier la configuration du blocage de l'accès public pour un compartiment S3.

Opérations d'API	Actions de politique	Description des actions de politique
UpdateBucketMetadataInventoryTableConfiguration	(Obligatoire) `s3:UpdateBucketMetadataInventoryTableConfiguration` `s3tables:CreateTableBucket` ,`s3tables:CreateNamespace` ,`s3tables:CreateTable` ,`s3tables:GetTable` ,`s3tables:PutTablePolicy` ,`s3tables:PutTableEncryption` , `kms:DescribeKey`	Nécessaire pour activer ou désactiver une table d'inventaire pour une configuration de table de métadonnées sur un bucket à usage général. Si vous souhaitez chiffrer votre table d'inventaire à l'aide d'un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), vous avez besoin d'autorisations supplémentaires dans votre politique de clés KMS. Pour de plus amples informations, veuillez consulter the section called "Autorisations pour les tables de métadonnées".
UpdateBucketMetadataJournalTableConfiguration	(Obligatoire) `s3:UpdateBucketMetadataJournalTableConfiguration`	Nécessaire pour activer ou désactiver l'expiration des enregistrements de table de journal pour une configuration de table de métadonnées dans un bucket à usage général.

Opérations d'objet et autorisations

Les opérations d'objet sont des opérations d'API S3 qui agissent sur le type de ressource de l'objet. Vous devez spécifier les actions de politique S3 pour les opérations d'objet dans des politiques basées sur les ressources (telles que des politiques de compartiment, des stratégies de point

d'accès, des stratégies de point d'accès multi-régions, des politiques de point de terminaison de VPC) ou dans des politiques basées sur l'identité IAM.

Dans les politiques, l'élément `Resource` doit être l'ARN de l'objet. Pour obtenir plus d'informations sur le format des éléments `Resource` et pour voir des exemples de politiques, consultez Opérations d'objet.

> **Note**
>
> - AWS KMS les actions de stratégie (`kms:GenerateDataKeyetkms:Decrypt`) ne s'appliquent qu'au type de AWS KMS ressource et doivent être spécifiées dans les politiques basées sur l'identité IAM et les politiques basées sur les AWS KMS ressources (politiques clés).AWS KMS Vous ne pouvez pas spécifier d'actions AWS KMS politiques dans les politiques basées sur les ressources S3, telles que les politiques de compartiment S3.
> - Lorsque vous utilisez des points d'accès pour contrôler l'accès aux opérations d'objet, vous pouvez utiliser des stratégies de point d'accès. Pour accorder des autorisations aux opérations d'objet dans les stratégies de point d'accès, notez ce qui suit :
>   - Dans les politiques de point d'accès qui accordent des autorisations pour les opérations sur les objets, l'`Resource`élément doit être celui ARNs destiné aux objets accessibles via un point d'accès. Pour obtenir plus d'informations sur le format des éléments `Resource` et pour voir des exemples de politiques, consultez Opérations d'objet dans les stratégies de point d'accès.
>   - Les opérations d'objet ne sont pas toutes prises en charge par les points d'accès. Pour de plus amples informations, veuillez consulter Compatibilité des points d'accès avec les opérations S3.
> - Les opérations d'objet ne sont pas toutes prises en charge par les points d'accès multi-régions. Pour de plus amples informations, veuillez consulter Compatibilité du point d'accès multi-régions avec les opérations S3.

Vous trouverez ci-dessous le mappage des opérations d'objet et des actions de politiques requises.

Opérations d'API	Actions de politique	Description des actions de politique
AbortMultipartUpload	(Obligatoire) `s3:AbortMultipartUpload`	Obligatoire pour abandonner un chargement partitionné.
CompleteMultipartUpload	(Obligatoire) `s3:PutObject`	Obligatoire pour finaliser un chargement partitionné.
	(Obligatoire sous condition) `kms:Decrypt`	Obligatoire si vous souhaitez effectuer un téléchargement en plusieurs parties pour un objet chiffré par clé géré par le AWS KMS client.
CopyObject	Pour l'objet source :	Pour l'objet source :
	(Obligatoire) `s3:GetObject` ou `s3:GetObjectVersion`	• `s3:GetObject` : obligatoire si vous souhaitez copier un objet depuis le compartiment source sans spécifier `versionId` dans la demande. • `s3:GetObjectVersion` : obligatoire si vous souhaitez copier une version spécifique d'un objet depuis le compartiment source en spécifiant `versionId` dans la demande.
	(Obligatoire sous condition) `kms:Decrypt`	Obligatoire si vous souhaitez copier un objet chiffré par clé géré par le AWS KMS client depuis le compartiment source.

Opérations d'API	Actions de politique	Description des actions de politique
	Pour l'objet de destination :	Pour l'objet de destination :
	(Obligatoire) `s3:PutObject`	Obligatoire pour placer l'objet copié dans le compartiment de destination.
	(Obligatoire sous condition) `s3:PutObjectAcl`	Obligatoire si vous souhaitez placer l'objet copié avec la liste de contrôle d'accès (ACL) de cet objet dans le compartiment de destination lorsque vous effectuez une demande `CopyObject` .
	(Obligatoire sous condition) `s3:PutObjectTagging`	Obligatoire si vous souhaitez placer l'objet copié avec le balisage d'objet dans le compartiment de destination lorsque vous effectuez une demande `CopyObject` .
	(Obligatoire sous condition) `kms:GenerateDataKey`	Obligatoire si vous souhaitez chiffrer l'objet copié à l'aide d'une clé gérée par le AWS KMS client et le placer dans le compartiment de destination.
	(Obligatoire sous condition) `s3:PutObjectRetention`	Obligatoire si vous souhaitez définir une configuration de rétention du verrouillage d'objet au nouvel objet.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `s3:PutObjectLegalHold`	Obligatoire si vous souhaitez appliquer une conservation légale du verrouillage d'objet au niveau du nouvel objet.
CreateMultipartUpload	(Obligatoire) `s3:PutObject`	Obligatoire pour créer un chargement partitionné.
	(Obligatoire sous condition) `s3:PutObjectAcl`	Obligatoire si vous souhaitez définir les autorisations d'une liste de contrôle d'accès (ACL) pour l'objet chargé.
	(Obligatoire sous condition) `s3:PutObjectTagging`	Obligatoire si vous souhaitez ajouter des balises à l'objet chargé.
	(Obligatoire sous condition) `kms:GenerateDataKey`	Obligatoire si vous souhaitez utiliser une clé gérée par le AWS KMS client pour chiffrer un objet lorsque vous lancez un téléchargement partitionné.
	(Obligatoire sous condition) `s3:PutObjectRetention`	Obligatoire si vous souhaitez définir une configuration de rétention du verrouillage d'objet pour l'objet chargé.
	(Obligatoire sous condition) `s3:PutObjectLegalHold`	Obligatoire si vous souhaitez appliquer une conservation légale du verrouillage d'objet à l'objet chargé.

Opérations d'API	Actions de politique	Description des actions de politique
DeleteObject	(Obligatoire) `s3:DeleteObject` ou `s3:DeleteObjectVersion`	• `s3:DeleteObject` : obligatoire si vous souhaitez supprimer un objet sans spécifier `versionId` dans la demande. • `s3:DeleteObjectVersion` : obligatoire si vous souhaitez supprimer une version spécifique d'un objet en spécifiant `versionId` dans la demande.
	(Obligatoire sous condition) `s3:BypassGovernanceRetention`	Obligatoire si vous souhaitez supprimer un objet protégé par le mode de gouvernance pour la rétention du verrouillage d'objet.
DeleteObjects	(Obligatoire) `s3:DeleteObject` ou `s3:DeleteObjectVersion`	• `s3:DeleteObject` : obligatoire si vous souhaitez supprimer un objet sans spécifier `versionId` dans la demande. • `s3:DeleteObjectVersion` : obligatoire si vous souhaitez supprimer une version spécifique d'un objet en spécifiant `versionId` dans la demande.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `s3:BypassGovernanceRetention`	Obligatoire si vous souhaitez supprimer des objets protégés par le mode de gouvernance pour la rétention du verrouillage d'objet.
DeleteObjectTagging	(Obligatoire) `s3:DeleteObjectTagging` ou `s3:DeleteObjectVersionTagging`	• `s3:DeleteObjectTagging` : obligatoire si vous souhaitez supprimer l'ensemble de balises complet d'un objet sans spécifier `versionId` dans la demande. • `s3:DeleteObjectVersionTagging` : obligatoire si vous souhaitez supprimer les balises d'une version d'objet spécifique en spécifiant `versionId` dans la demande.
GetObject	(Obligatoire) `s3:GetObject` ou `s3:GetObjectVersion`	• `s3:GetObject` : obligatoire si vous souhaitez obtenir un objet sans spécifier `versionId` dans la demande. • `s3:GetObjectVersion` : obligatoire si vous souhaitez obtenir une version spécifique d'un objet en spécifiant `versionId` dans la demande.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `kms:Decrypt`	Obligatoire si vous souhaitez obtenir et déchiffrer un objet chiffré par clé géré par le AWS KMS client.
	(Obligatoire sous condition) `s3:GetObjectTagging`	Obligatoire si vous souhaitez obtenir l'ensemble de balises d'un objet lorsque vous effectuez une demande `GetObject` .
	(Obligatoire sous condition) `s3:GetObjectLegalHold`	Obligatoire si vous souhaitez obtenir le statut actuel de la conservation légale du verrouillage d'un objet.
	(Obligatoire sous condition) `s3:GetObjectRetention`	Obligatoire si vous souhaitez récupérer les paramètres de rétention du verrouillage d'un objet.
GetObjectAcl	(Obligatoire) `s3:GetObjectAcl` ou `s3:GetObjectVersionAcl`	• `s3:GetObjectAcl` : obligatoire si vous souhaitez obtenir la liste de contrôle d'accès (ACL) d'un objet sans spécifier `versionId` dans la demande. • `s3:GetObjectVersionAcl` : obligatoire si vous souhaitez obtenir la liste de contrôle d'accès (ACL) d'un objet en spécifiant `versionId` dans la demande.

Opérations d'API	Actions de politique	Description des actions de politique
GetObjectAttributes	(Obligatoire) `s3:GetObject` ou `s3:GetObjectVersion`	• `s3:GetObject` : obligatoire si vous souhaitez récupérer les attributs associés à un objet sans spécifier `versionId` dans la demande. • `s3:GetObjectVersion` : obligatoire si vous souhaitez récupérer les attributs liés à une version d'objet spécifique en spécifiant `versionId` dans la demande.
	(Obligatoire sous condition) `kms:Decrypt`	Obligatoire si vous souhaitez récupérer les attributs associés à un objet chiffré par clé géré par le AWS KMS client.
GetObjectLegalHold	(Obligatoire) `s3:GetObjectLegalHold`	Obligatoire pour obtenir le statut actuel de la conservation légale du verrouillage d'un objet.
GetObjectRetention	(Obligatoire) `s3:GetObjectRetention`	Obligatoire pour récupérer les paramètres de rétention du verrouillage d'un objet.

Opérations d'API	Actions de politique	Description des actions de politique
GetObjectTagging	(Obligatoire) `s3:GetObjectTagging` ou `s3:GetObjectVersionTagging`	• `s3:GetObjectTagging` : obligatoire si vous souhaitez obtenir l'ensemble de balises d'un objet sans spécifier `versionId` dans la demande. • `s3:GetObjectVersionTagging` : obligatoire si vous souhaitez obtenir les balises d'une version d'objet spécifique en spécifiant `versionId` dans la demande.
GetObjectTorrent	(Obligatoire) `s3:GetObject`	Obligatoire pour renvoyer les fichiers torrent d'un objet.
HeadObject	(Obligatoire) `s3:GetObject`	Obligatoire pour récupérer les métadonnées d'un objet sans renvoyer l'objet lui-même.
	(Obligatoire sous condition) `s3:GetObjectLegalHold`	Obligatoire si vous souhaitez obtenir le statut actuel de la conservation légale du verrouillage d'un objet.
	(Obligatoire sous condition) `s3:GetObjectRetention`	Obligatoire si vous souhaitez récupérer les paramètres de rétention du verrouillage d'un objet.
ListMultipartUploads	(Obligatoire) `s3:ListBucketMultipartUploads`	Obligatoire pour répertorier les chargements partitionnés en cours dans un compartiment.

Opérations d'API	Actions de politique	Description des actions de politique
ListParts	(Obligatoire) `s3:ListMultipartUploadParts`	Obligatoire pour répertorier les parties qui ont été chargées au cours d'un chargement partitionné spécifique.
	(Obligatoire sous condition) `kms:Decrypt`	Obligatoire si vous souhaitez répertorier les parties d'un téléchargement en plusieurs parties chiffré par clé gérée par le AWS KMS client.
PutObject	(Obligatoire) `s3:PutObject`	Obligatoire pour placer un objet.
	(Obligatoire sous condition) `s3:PutObjectAcl`	Obligatoire si vous souhaitez placer la liste de contrôle d'accès (ACL) d'un objet lorsque vous effectuez une demande `PutObject` .
	(Obligatoire sous condition) `s3:PutObjectTagging`	Obligatoire si vous souhaitez placer le balisage d'un objet lorsque vous effectuez une demande `PutObject` .
	(Obligatoire sous condition) `kms:GenerateDataKey`	Obligatoire si vous souhaitez chiffrer un objet à l'aide d'une clé gérée par AWS KMS le client.
	(Obligatoire sous condition) `s3:PutObjectRetention`	Obligatoire si vous souhaitez définir une configuration de rétention du verrouillage d'objet au niveau d'un objet.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `s3:PutObjectLegalHold`	Obligatoire si vous souhaitez appliquer une configuration de conservation légale du verrouillage d'objet à un objet spécifié.
PutObjectAcl	(Obligatoire) `s3:PutObjectAcl` ou `s3:PutObjectVersionAcl`	• `s3:PutObjectAcl` : obligatoire si vous souhaitez définir les autorisations de liste de contrôle d'accès (ACL) pour un objet nouveau ou existant sans spécifier `versionId` dans la demande. • `s3:PutObjectVersionAcl` : obligatoire si vous souhaitez définir les autorisations de liste de contrôle d'accès (ACL) pour un objet nouveau ou existant en spécifiant `versionId` dans la demande.
PutObjectLegalHold	(Obligatoire) `s3:PutObjectLegalHold`	Obligatoire pour appliquer une configuration de la conservation légale du verrouillage d'objet à un objet.
PutObjectRetention	(Obligatoire) `s3:PutObjectRetention`	Obligatoire pour appliquer une configuration de rétention du verrouillage d'objet à un objet.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `s3:BypassGovernanceRetention`	Obligatoire si vous souhaitez contourner le mode de gouvernance d'une configuration de rétention du verrouillage d'objet.
PutObjectTagging	(Obligatoire) `s3:PutObjectTagging` ou `s3:PutObjectVersionTagging`	• `s3:PutObjectTagging` : obligatoire si vous souhaitez définir l'ensemble de balises fourni pour un objet qui existe déjà dans un compartiment sans spécifier `versionId` dans la demande. • `s3:PutObjectVersionTagging` : obligatoire si vous souhaitez définir l'ensemble de balises fourni pour un objet qui existe déjà dans un compartiment en spécifiant `versionId` dans la demande.
RestoreObject	(Obligatoire) `s3:RestoreObject`	Obligatoire pour restaurer une copie d'un objet archivé.
SelectObjectContent	(Obligatoire) `s3:GetObject`	Obligatoire pour filtrer le contenu d'un objet S3 en fonction d'une instruction SQL (Structured Query Language) simple.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `kms:Decrypt`	Obligatoire si vous souhaitez filtrer le contenu d'un objet S3 chiffré à l'aide d'une clé gérée par AWS KMS le client.
UploadPart	(Obligatoire) `s3:PutObject`	Obligatoire pour charger une partie d'un chargement partitionné.
	(Obligatoire sous condition) `kms:GenerateDataKey`	Obligatoire si vous souhaitez ajouter une partie de téléchargement et la chiffrer à l'aide d'une clé gérée par AWS KMS le client.
UploadPartCopy	Pour l'objet source :	Pour l'objet source :
	(Obligatoire) `s3:GetObject` ou `s3:GetObjectVersion`	• `s3:GetObject` : obligatoire si vous souhaitez copier un objet depuis le compartiment source sans spécifier `versionId` dans la demande. • `s3:GetObjectVersion` : obligatoire si vous souhaitez copier une version spécifique d'un objet depuis le compartiment source en spécifiant `versionId` dans la demande.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `kms:Decrypt`	Obligatoire si vous souhaitez copier un objet chiffré par clé géré par le AWS KMS client depuis le compartiment source.
	Pour la partie de destination :	Pour la partie de destination :
	(Obligatoire) `s3:PutObject`	Obligatoire pour charger une partie du chargement partition né dans le compartiment de destination.
	(Obligatoire sous condition) `kms:GenerateDataKey`	Obligatoire si vous souhaitez chiffrer une pièce à l'aide d'une clé gérée par le AWS KMS client lorsque vous la chargez dans le compartiment de destination.

Point d'accès pour les opérations et autorisations de buckets à usage général

Les opérations de point d'accès sont des opérations d'API S3 qui agissent sur le type de ressource `accesspoint`. Vous devez spécifier les actions de politique S3 pour les opérations de point d'accès dans les politiques basées sur l'identité IAM, et non dans les politiques de compartiment ou les stratégies de point d'accès.

Dans les politiques, l'élément `Resource` doit être l'ARN d'`accesspoint`. Pour obtenir plus d'informations sur le format des éléments `Resource` et pour voir des exemples de politiques, consultez Point d'accès pour les opérations de godet à usage général.

> **Note**
>
> Si vous souhaitez utiliser des points d'accès pour contrôler l'accès aux opérations de compartiment ou d'objet, notez ce qui suit :

- Pour utiliser des points d'accès afin de contrôler l'accès aux opérations de compartiment, consultez Opérations relatives aux compartiments dans les politiques relatives aux points d'accès pour les compartiments à usage général.
- Pour utiliser des points d'accès afin de contrôler l'accès aux opérations d'objet, consultez Opérations d'objet dans les stratégies de point d'accès.
- Pour plus d'informations sur la configuration de stratégies de point d'accès, consultez Configuration des politiques IAM pour l'utilisation des points d'accès.

Vous trouverez ci-dessous le mappage des opérations de point d'accès et des actions de politiques requises.

Opérations d'API	Actions de politique	Description des actions de politique
CreateAccessPoint	(Obligatoire) `s3:CreateAccessPoint`	Obligatoire pour créer un point d'accès associé à un compartiment S3.
DeleteAccessPoint	(Obligatoire) `s3:DeleteAccessPoint`	Obligatoire pour supprimer un point d'accès.
DeleteAccessPointPolicy	(Obligatoire) `s3:DeleteAccessPointPolicy`	Obligatoire pour supprimer une stratégie de point d'accès.
GetAccessPointPolicy	(Obligatoire) `s3:GetAccessPointPolicy`	Obligatoire pour récupérer une stratégie de point d'accès.
GetAccessPointPolicyStatus	(Obligatoire) `s3:GetAccessPointPolicyStatus`	Obligatoire pour récupérer les informations indiquant si le point d'accès spécifié dispose actuellement d'une stratégie autorisant l'accès public.
PutAccessPointPolicy	(Obligatoire) `s3:PutAccessPointPolicy`	Obligatoire pour placer une stratégie de point d'accès.

Opérations de point d'accès Object Lambda et autorisations

Les opérations de point d'accès Object Lambda sont des opérations d'API S3 qui agissent sur le type de ressource `objectlambdaaccesspoint`. Pour plus d'informations sur la configuration de politiques pour les opérations de point d'accès Object Lambda, consultez Configuration des politiques IAM pour les points d'accès Object Lambda.

Vous trouverez ci-dessous le mappage des opérations de point d'accès Object Lambda et des actions de politiques requises.

Opérations d'API	Actions de politique	Description des actions de politique
CreateAccessPointForObjectLambda	(Obligatoire) `s3:CreateAccessPointForObjectLambda`	Obligatoire pour créer un point d'accès Object Lambda.
DeleteAccessPointForObjectLambda	(Obligatoire) `s3:DeleteAccessPointForObjectLambda`	Obligatoire pour supprimer un point d'accès Object Lambda spécifié.
DeleteAccessPointPolicyForObjectLambda	(Obligatoire) `s3:DeleteAccessPointPolicyForObjectLambda`	Obligatoire pour supprimer la stratégie au niveau d'un point d'accès Object Lambda spécifié.
GetAccessPointConfigurationForObjectLambda	(Obligatoire) `s3:GetAccessPointConfigurationForObjectLambda`	Obligatoire pour récupérer la configuration du point d'accès Object Lambda.
GetAccessPointForObjectLambda	(Obligatoire) `s3:GetAccessPointForObjectLambda`	Obligatoire pour récupérer des informations sur le point d'accès Object Lambda.
GetAccessPointPolicyForObjectLambda	(Obligatoire) `s3:GetAccessPointPolicyForObjectLambda`	Obligatoire pour renvoyer la politique de point d'accès associée au point d'accès Object Lambda spécifié.

Opérations d'API	Actions de politique	Description des actions de politique
GetAccessPointPolicyStatusForObjectLambda	(Obligatoire) `s3:GetAccessPointPolicyStatusForObjectLambda`	Obligatoire pour renvoyer le statut d'une politique de point d'accès Object Lambda spécifique.
PutAccessPointConfigurationForObjectLambda	(Obligatoire) `s3:PutAccessPointConfigurationForObjectLambda`	Obligatoire pour définir la configuration du point d'accès Object Lambda.
PutAccessPointPolicyForObjectLambda	(Obligatoire) `s3:PutAccessPointPolicyForObjectLambda`	Obligatoire pour associer une stratégie d'accès à un point d'accès Object Lambda spécifié.

Opérations de point d'accès multi-régions et autorisations

Les opérations de point d'accès multi-régions sont des opérations d'API S3 qui agissent sur le type de ressource `multiregionaccesspoint`. Pour plus d'informations sur la configuration de stratégies pour les opérations de points d'accès multi-régions, consultez Exemples de politique de point d'accès multi-régions.

Voici le mappage des opérations de point d'accès multi-régions et des actions de politique requises.

Opérations d'API	Actions de politique	Description des actions de politique
CreateMultiRegionAccessPoint	(Obligatoire) `s3:CreateMultiRegionAccessPoint`	Obligatoire pour créer un point d'accès multi-régions et l'associer à des compartiments S3.
DeleteMultiRegionAccessPoint	(Obligatoire) `s3:DeleteMultiRegionAccessPoint`	Obligatoire pour supprimer un point d'accès multi-régions.

Opérations d'API	Actions de politique	Description des actions de politique
DescribeMultiRegionAccessPointOperation	(Obligatoire) `s3:DescribeMultiRegionAccessPointOperation`	Obligatoire pour récupérer le statut d'une demande asynchrone pour gérer un point d'accès multi-régions.
GetMultiRegionAccessPoint	(Obligatoire) `s3:GetMultiRegionAccessPoint`	Obligatoire pour renvoyer des informations de configuration sur le point d'accès multi-régions spécifié.
GetMultiRegionAccessPointPolicy	(Obligatoire) `s3:GetMultiRegionAccessPointPolicy`	Obligatoire pour renvoyer la stratégie de contrôle d'accès du point d'accès multi-régions spécifié.
GetMultiRegionAccessPointPolicyStatus	(Obligatoire) `s3:GetMultiRegionAccessPointPolicyStatus`	Obligatoire pour renvoyer le statut de la stratégie d'un point d'accès multi-régions spécifique, indiquant si le point d'accès multi-régions spécifié dispose d'une stratégie de contrôle d'accès qui autorise l'accès public.
GetMultiRegionAccessPointRoutes	(Obligatoire) `s3:GetMultiRegionAccessPointRoutes`	Obligatoire pour renvoyer la configuration de routage pour un point d'accès multi-régions.
PutMultiRegionAccessPointPolicy	(Obligatoire) `s3:PutMultiRegionAccessPointPolicy`	Obligatoire pour mettre à jour la stratégie de contrôle d'accès du point d'accès multi-régions spécifié.

Opérations d'API	Actions de politique	Description des actions de politique
SubmitMultiRegionAccessPointRoutes	(Obligatoire) `s3:SubmitMultiRegionAccessPointRoutes`	Obligatoire pour soumettre une configuration de routage mise à jour pour un point d'accès multi-régions.

Opérations relatives aux tâches par lots et autorisations

Les opérations relatives aux tâches par lots (opérations par lot) sont des opérations d'API S3 qui agissent sur le type de ressource `job`. Vous devez spécifier les actions de politique S3 pour les opérations relatives aux tâches par lots dans les politiques basées sur l'identité IAM, et non dans les politiques de compartiment.

Dans les politiques, l'élément `Resource` doit être l'ARN d'`job`. Pour obtenir plus d'informations sur le format des éléments `Resource` et pour voir des exemples de politiques, consultez Opérations relatives aux tâches par lots.

Vous trouverez ci-dessous le mappage des opérations relatives aux tâches par lots et des actions de politique requises.

Opérations d'API	Actions de politique	Description des actions de politique
DeleteJobTagging	(Obligatoire) `s3:DeleteJobTagging`	Obligatoire pour supprimer des balises d'une tâche d'opérations par lot S3 existante.
DescribeJob	(Obligatoire) `s3:DescribeJob`	Obligatoire pour récupérer les paramètres de configuration et le statut d'une tâche d'opérations par lot.
GetJobTagging	(Obligatoire) `s3:GetJobTagging`	Obligatoire pour renvoyer l'ensemble de balises d'une

Opérations d'API	Actions de politique	Description des actions de politique
		tâche d'opérations par lot S3 existante.
PutJobTagging	(Obligatoire) `s3:PutJobTagging`	Obligatoire pour placer ou remplacer des balises au niveau d'une tâche d'opérations par lot S3 existante.
UpdateJobPriority	(Obligatoire) `s3:UpdateJobPriority`	Obligatoire pour mettre à jour la priorité d'une tâche existante.
UpdateJobStatus	(Obligatoire) `s3:UpdateJobStatus`	Obligatoire pour mettre à jour le statut de la tâche spécifiée.

Opérations de configuration S3 Storage Lens et autorisations

Les opérations de configuration S3 Storage Lens sont des opérations d'API S3 qui agissent sur le type de ressource `storagelensconfiguration`. Pour plus d'informations sur les opérations de configuration S3 Storage Lens, consultez Définition d'autorisations Amazon S3 Storage Lens.

Vous trouverez ci-dessous le mappage des opérations de configuration S3 Storage Lens et des actions de politique requises.

Opérations d'API	Actions de politique	Description des actions de politique
DeleteStorageLensConfiguration	(Obligatoire) `s3:DeleteStorageLensConfiguration`	Obligatoire pour supprimer la configuration S3 Storage Lens.
DeleteStorageLensConfigurationTagging	(Obligatoire) `s3:DeleteStorageLensConfigurationTagging`	Obligatoire pour supprimer les balises de configuration S3 Storage Lens.

Opérations d'API	Actions de politique	Description des actions de politique
GetStorageLensConfiguration	(Obligatoire) `s3:GetStorageLensConfiguration`	Obligatoire pour obtenir la configuration S3 Storage Lens.
GetStorageLensConfigurationTagging	(Obligatoire) `s3:GetStorageLensConfigurationTagging`	Obligatoire pour obtenir les balises de configuration S3 Storage Lens.
PutStorageLensConfigurationTagging	(Obligatoire) `s3:PutStorageLensConfigurationTagging`	Obligatoire pour placer ou remplacer des balises au niveau d'une configuration Amazon S3 Storage Lens existante.

Opérations des groupes S3 Storage Lens et autorisations

Les opérations des groupes S3 Storage Lens sont des opérations d'API S3 qui agissent sur le type de ressource `storagelensgroup`. Pour plus d'informations sur la configuration de S3 Storage Lens, consultez Autorisations pour les groupes Storage Lens.

Vous trouverez ci-dessous le mappage des opérations des groupes S3 Storage Lens et des actions de politique requises.

Opérations d'API	Actions de politique	Description des actions de politique
DeleteStorageLensGroup	(Obligatoire) `s3:DeleteStorageLensGroup`	Obligatoire pour supprimer un groupe S3 Storage Lens existant.
GetStorageLensGroup	(Obligatoire) `s3:GetStorageLensGroup`	Obligatoire pour récupérer les détails de configuration d'un groupe S3 Storage Lens.

Opérations d'API	Actions de politique	Description des actions de politique
UpdateStorageLensGroup	(Obligatoire) `s3:UpdateStorageLensGroup`	Obligatoire pour mettre à jour le groupe S3 Storage Lens existant.
CreateStorageLensGroup	(Obligatoire) `s3:CreateStorageLensGroup`	Nécessaire pour créer un nouveau groupe Storage Lens.
CreateStorageLensGroup, TagResource	(Obligatoire)`s3:CreateStorageLensGroup` , `s3:TagResource`	Nécessaire pour créer un nouveau groupe Storage Lens avec des balises.
ListStorageLensGroups	(Obligatoire) `s3:ListStorageLensGroups`	Obligatoire pour répertorier tous les groupes de lentilles de stockage de votre région d'origine.
ListTagsForResource	(Obligatoire) `s3:ListTagsForResource`	Obligatoire pour répertorier les balises ajoutées à votre groupe Storage Lens.
TagResource	(Obligatoire) `s3:TagResource`	Nécessaire pour ajouter ou mettre à jour une étiquette de groupe Storage Lens pour un groupe Storage Lens existant.
UntagResource	(Obligatoire) `s3:UntagResource`	Nécessaire pour supprimer une balise d'un groupe Storage Lens.

Opérations et autorisations de l'instance S3 Access Grants

Les opérations d'instance S3 Access Grants sont des opérations d'API S3 qui opèrent sur le type de `accessgrantsinstance` ressource. Une instance S3 Access Grants est un conteneur logique pour

vos autorisations d'accès. Pour plus d'informations sur l'utilisation des instances S3 Access Grants, consultezUtilisation des instances d'autorisations d'accès S3.

Voici le mappage des opérations de configuration de l'instance S3 Access Grants et des actions politiques requises.

Opérations d'API	Actions de politique	Description des actions de politique
AssociateAccessGrantsIdentityCenter	(Obligatoire) `s3:AssociateAccessGrantsIdentityCenter`	Nécessaire pour associer une AWS IAM Identity Center instance à votre instance S3 Access Grants, vous permettant ainsi de créer des autorisations d'accès pour les utilisateurs et les groupes dans votre répertoire d'identité d'entreprise. Vous devez également disposer des autorisations suivantes : `sso:CreateApplication` , `sso:PutApplicationGrant` et `sso:PutApplicationAuthenticationMethod` .
CreateAccessGrantsInstance	(Obligatoire) `s3:CreateAccessGrantsInstance`	Nécessaire pour créer une instance S3 Access Grants (`accessgrantsinstance` ressource) qui est un conteneur pour vos autorisations d'accès individuelles. Pour associer une AWS IAM Identity Center instance à votre instance S3 Access

Opérations d'API	Actions de politique	Description des actions de politique
		Grants, vous devez également disposer des `sso:PutApplicationAuthenticationMethod` autorisations `sso:DescribeInstance` `sso:CreateApplication` `sso:PutApplicationGrant` ,, et.
DeleteAccessGrantsInstance	(Obligatoire) `s3:DeleteAccessGrantsInstance`	Nécessaire pour supprimer une instance S3 Access Grants (`accessgrantsinstance` ressource) Région AWS d'un compte.
DeleteAccessGrantsInstanceResourcePolicy	(Obligatoire) `s3:DeleteAccessGrantsInstanceResourcePolicy`	Nécessaire pour supprimer une politique de ressources pour votre instance S3 Access Grants.
DissociateAccessGrantsIdentityCenter	(Obligatoire) `s3:DissociateAccessGrantsIdentityCenter`	Nécessaire pour dissocier une AWS IAM Identity Center instance de votre instance S3 Access Grants. Vous devez également disposer des autorisations suivantes : `sso:DeleteApplication`
GetAccessGrantsInstance	(Obligatoire) `s3:GetAccessGrantsInstance`	Nécessaire pour récupérer l'instance S3 Access Grants pour une instance Région AWS intégrée à votre compte.

Opérations d'API	Actions de politique	Description des actions de politique
GetAccessGrantsInstanceForPrefix	(Obligatoire) `s3:GetAccessGrantsInstanceForPrefix`	Nécessaire pour récupérer l'instance S3 Access Grants qui contient un préfixe particulier.
GetAccessGrantsInstanceResourcePolicy	(Obligatoire) `s3:GetAccessGrantsInstanceResourcePolicy`	Obligatoire pour renvoyer la politique de ressources de votre instance S3 Access Grants.
ListAccessGrantsInstances	(Obligatoire) `s3:ListAccessGrantsInstances`	Obligatoire pour renvoyer la liste des instances S3 Access Grants de votre compte.
PutAccessGrantsInstanceResourcePolicy	(Obligatoire) `s3:PutAccessGrantsInstanceResourcePolicy`	Nécessaire pour mettre à jour la politique de ressources de l'instance S3 Access Grants.

S3 Access accorde des autorisations et des opérations de localisation

Les opérations de localisation des autorisations d'accès S3 sont des opérations d'API S3 qui opèrent sur le type de `accessgrantslocation` ressource. Pour plus d'informations sur l'utilisation des emplacements S3 Access Grants, consultezUtilisation des emplacements d'autorisations d'accès S3.

Vous trouverez ci-dessous le mappage des opérations de configuration de l'emplacement des subventions d'accès S3 et des actions politiques requises.

Opérations d'API	Actions de politique	Description des actions de politique
CreateAccessGrantsLocation	(Obligatoire) `s3:CreateAccessGrantsLocation`	Nécessaire pour enregistrer un emplacement dans votre instance S3 Access Grants (créer une `accessgrantslocation` ressource

Opérations d'API	Actions de politique	Description des actions de politique
		). Vous devez également disposer de l'autorisation suivante pour le rôle IAM spécifié : `iam:PassRole`
DeleteAccessGrantsLocation	(Obligatoire) `s3:DeleteAccessGrantsLocation`	Nécessaire pour supprimer un emplacement enregistré de votre instance S3 Access Grants.
GetAccessGrantsLocation	(Obligatoire) `s3:GetAccessGrantsLocation`	Nécessaire pour récupérer les détails d'un emplacement spécifique enregistré dans votre instance S3 Access Grants.
ListAccessGrantsLocations	(Obligatoire) `s3:ListAccessGrantsLocations`	Obligatoire pour renvoyer une liste des emplacements enregistrés dans votre instance S3 Access Grants.
UpdateAccessGrantsLocation	(Obligatoire) `s3:UpdateAccessGrantsLocation`	Nécessaire pour mettre à jour le rôle IAM d'un emplacement enregistré dans votre instance S3 Access Grants.

Les subventions d'accès S3 octroient des opérations et des autorisations

Les opérations d'octroi de subventions d'accès S3 sont des opérations d'API S3 qui opèrent sur le type de `accessgrant` ressource. Pour plus d'informations sur l'utilisation de subventions individuelles à l'aide de S3 Access Grants, consultezOctroi d'autorisations avec les autorisations d'accès S3.

Voici le mappage des opérations de configuration des subventions d'accès S3 et des actions politiques requises.

Opérations d'API	Actions de politique	Description des actions de politique
CreateAccessGrant	(Obligatoire) `s3:CreateAccessGrant`	Nécessaire pour créer une autorisation individuelle (`accessgrant` ressource) pour un utilisateur ou un groupe dans votre instance S3 Access Grants. Vous devez également disposer des autorisations suivantes : Pour n'importe quelle identité de répertoire, `sso:DescribeInstance` et `sso:DescribeApplication` Pour les utilisateurs de l'annuaire : `identitystore:DescribeUser`
DeleteAccessGrant	(Obligatoire) `s3:DeleteAccessGrant`	Nécessaire pour supprimer une autorisation d'accès individuelle (`accessgrant` ressource) de votre instance S3 Access Grants.
GetAccessGrant	(Obligatoire) `s3:GetAccessGrant`	Nécessaire pour obtenir les détails d'une autorisation d'accès individuelle dans votre instance S3 Access Grants.
ListAccessGrants	(Obligatoire) `s3:ListAccessGrants`	Obligatoire pour renvoyer une liste des autorisations

Opérations d'API	Actions de politique	Description des actions de politique
		d'accès individuelles dans votre instance S3 Access Grants.
ListCallerAccessGrants	(Obligatoire) `s3:ListCallerAccessGrants`	Obligatoire pour répertorier les autorisations d'accès qui accordent à l'appelant l'accès aux données Amazon S3 via S3 Access Grants.

Opérations de compte et autorisations

Les opérations de compte sont des opérations d'API S3 qui agissent au niveau du compte. Le compte n'est pas un type de ressource défini par Amazon S3. Vous devez spécifier les actions de politique S3 pour les opérations de compte dans les politiques basées sur l'identité IAM, et non dans les politiques de compartiment.

Dans les politiques, l'élément `Resource` doit être `"*"`. Pour plus d'informations sur les exemples de politiques, consultez Opérations de compte.

Vous trouverez ci-dessous le mappage des opérations de compte et des actions de politique requises.

Opérations d'API	Actions de politique	Description des actions de politique
CreateJob	(Obligatoire) `s3:CreateJob`	Obligatoire pour créer une tâche d'opérations par lot S3.
CreateStorageLensGroup	(Obligatoire) `s3:CreateStorageLensGroup`	Nécessaire pour créer un nouveau groupe S3 Storage Lens et l'associer à l' Compte AWS ID spécifié.

Opérations d'API	Actions de politique	Description des actions de politique
	(Obligatoire sous condition) `s3:TagResource`	Obligatoire si vous souhaitez créer un groupe S3 Storage Lens avec AWS des balises de ressources.
DeletePublicAccessBlock (au niveau du compte)	(Obligatoire) `s3:PutAccountPublicAccessBlock`	Obligatoire pour supprimer la configuration du blocage de l'accès public d'un Compte AWS.
GetAccessPoint	(Obligatoire) `s3:GetAccessPoint`	Obligatoire pour récupérer des informations de configuration sur le point d'accès.
GetAccessPointPolicy (au niveau du compte)	(Obligatoire) `s3:GetAccountPublicAccessBlock`	Obligatoire pour récupérer la configuration du blocage de l'accès public pour un Compte AWS.
ListAccessPoints	(Obligatoire) `s3:ListAccessPoints`	Obligatoire pour répertorier les points d'accès d'un compartiment S3 appartenant à un Compte AWS.
ListAccessPointsForObjectLambda	(Obligatoire) `s3:ListAccessPointsForObjectLambda`	Obligatoire pour répertorier les points d'accès Object Lambda.
ListBuckets	(Obligatoire) `s3:ListAllMyBuckets`	Obligatoire pour renvoyer une liste de tous les compartiments appartenant à l'expéditeur authentifié de la demande.

Opérations d'API	Actions de politique	Description des actions de politique
ListJobs	(Obligatoire) `s3:ListJobs`	Obligatoire pour répertorier les tâches en cours et les tâches qui se sont terminées récemment.
ListMultiRegionAccessPoints	(Obligatoire) `s3:ListMultiRegionAccessPoints`	Obligatoire pour renvoyer une liste des points d'accès multi-régions actuellement associés au Compte AWS spécifié.
ListStorageLensConfigurations	(Obligatoire) `s3:ListStorageLensConfigurations`	Nécessaire pour obtenir une liste des configurations S3 Storage Lens pour un Compte AWS.
ListStorageLensGroups	(Obligatoire) `s3:ListStorageLensGroups`	Obligatoire pour répertorier tous les groupes S3 Storage Lens dans la Région AWS d'origine.
PutPublicAccessBlock (au niveau du compte)	(Obligatoire) `s3:PutAccountPublicAccessBlock`	Obligatoire pour créer ou modifier la configuration du blocage de l'accès public pour un Compte AWS.
PutStorageLensConfiguration	(Obligatoire) `s3:PutStorageLensConfiguration`	Obligatoire pour placer une configuration S3 Storage Lens.

Politiques, stratégies et autorisations dans Amazon S3

Cette page fournit un aperçu des politiques relatives aux compartiments et aux utilisateurs dans Amazon S3 et décrit les éléments de base d'une politique AWS Identity and Access Management

(IAM). Chaque élément répertorié renvoie vers des informations complémentaires sur cet élément et des exemples de son utilisation.

Pour obtenir la liste complète des actions, des ressources et des conditions Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Une stratégie de base contient les éléments suivants :

- Resource : compartiment, objet, point d'accès ou tâche Amazon S3 auxquels s'applique la politique. Utilisez l'Amazon Resource Name (ARN) du compartiment, de l'objet, du point d'accès ou de la tâche pour identifier la ressource.

  Exemple d'opérations au niveau du compartiment :

  `"Resource": "arn:aws:s3:::bucket_name"`

  Exemples d'opérations au niveau de l'objet :

  - `"Resource": "arn:aws:s3:::bucket_name/*"` pour tous les objets du compartiment.
  - `"Resource": "arn:aws:s3:::bucket_name/prefix/*"` pour les objets placés sous un certain préfixe dans le compartiment.

  Pour de plus amples informations, veuillez consulter Ressources de politique pour Amazon S3.
- Actions : pour chaque ressource, Amazon S3 prend en charge un ensemble d'opérations. Vous identifiez les opérations de ressource que vous accordez (ou refusez) en utilisant des mots clés d'action.

  Par exemple, l'autorisation `s3:ListBucket` permet à l'utilisateur d'exécuter l'opération Amazon S3 ListObjectsV2. (L'autorisation `s3:ListBucket` est un cas où le nom de l'action ne correspond pas directement au nom de l'opération.) Pour plus d'informations sur l'utilisation des actions Amazon S3, consultez Actions de politique pour Amazon S3. Pour obtenir la liste complète des actions Amazon S3, consultez Actions dans la Référence d'API Amazon Simple Storage Service.
- Effect : effet produit lorsque l'utilisateur demande l'action spécifique, qui peut être `Allow` ou `Deny`.

  Si vous n'accordez pas explicitement l'accès pour (autoriser) une ressource, l'accès est implicitement refusé. Vous pouvez également explicitement refuser l'accès à une ressource.

Vous pouvez le faire afin de vous assurer qu'un utilisateur n'y a pas accès, même si une stratégie différente accorde cet accès. Pour plus d'informations, consultez Éléments de politique JSON IAM : Effect dans le Guide de l'utilisateur IAM.

- Principal : compte ou utilisateur autorisé à accéder aux actions et aux ressources dans l'instruction. Dans une politique de compartiment, le principal est l'utilisateur, le compte, le service ou toute autre entité destinataire de cette autorisation. Pour de plus amples informations, veuillez consulter Principaux pour les politiques de compartiment.
- Condition – Conditions relatives au moment où une stratégie ou politique entre en vigueur. Vous pouvez utiliser AWS des clés larges et des clés spécifiques à Amazon S3 pour spécifier les conditions d'une politique d'accès Amazon S3. Pour de plus amples informations, veuillez consulter Exemples de politiques de compartiment utilisant des clés de condition.

L'exemple de politique de compartiment suivant montre les éléments `Effect`, `Principal`, `Action` et `Resource`. Cette politique accorde à *`Akua`*, utilisateur du compte *`123456789012`*, les autorisations Amazon S3 `s3:GetObject`, `s3:GetBucketLocation` et `s3:ListBucket` au niveau du compartiment *`amzn-s3-demo-bucket1`*.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "ExamplePolicy01",
    "Statement": [
        {
            "Sid": "ExampleStatement01",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Akua"
            },
            "Action": [
                "s3:GetObject",
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
        }
```

```
    ]
}
```

Pour obtenir des informations complètes sur le langage des politiques, consultez Politiques et autorisations dans IAM et Référence de politique JSON IAM dans le Guide de l'utilisateur IAM.

Délégation d'autorisations

Si une personne Compte AWS possède une ressource, elle peut accorder ces autorisations à une autre personne Compte AWS. Ce compte peut alors déléguer à ces utilisateurs, l'ensemble de ces autorisations ou un sous-ensemble de celles-ci. Cela s'appelle une délégation d'autorisations. Cependant, un compte qui reçoit des autorisations d'un autre compte ne peut pas déléguer cette autorisation intercomptes à un autre Compte AWS.

Propriété du compartiment et de l'objet Amazon S3

Les compartiments et les objets sont des ressources Amazon S3. Par défaut, seul le propriétaire de ressource peut accéder à ces ressources. Le propriétaire de la ressource fait référence à Compte AWS celui qui crée la ressource. Par exemple :

- Celui Compte AWS que vous utilisez pour créer des buckets et télécharger des objets possède ces ressources.
- Si vous chargez un objet à l'aide des informations d'identification d'utilisateur ou de rôle AWS Identity and Access Management (IAM), l' Compte AWS utilisateur ou le rôle auquel appartient l'utilisateur ou le rôle est propriétaire de l'objet.
- Un propriétaire de compartiment peut accorder à un autre Compte AWS (ou à des utilisateurs d'un autre compte) des autorisations inter-comptes pour charger des objets. Dans ce cas, le Compte AWS qui charge les objets est propriétaire de ceux-ci. Le propriétaire du compartiment n'a aucune autorisation sur les objets dont sont propriétaires d'autres comptes, à l'exception des cas suivants :
  - Le propriétaire du compartiment paie les factures. Le propriétaire du compartiment peut refuser l'accès aux objets ou supprimer des objets dans le compartiment, quel que soit le propriétaire de ces derniers.
  - Le propriétaire du compartiment peut archiver n'importe quel objet ou restaurer des objets archivés, quel qu'en soit le propriétaire. L'archivage fait référence à la classe de stockage utilisée pour stocker les objets. Pour plus d'informations, consultez Gestion du cycle de vie des objets.

Titularité et authentification de demande

Toutes les demandes à un compartiment sont soit authentifiées ou non authentifiées. Les demandes authentifiées doivent inclure une valeur de signature qui authentifie l'expéditeur de la demande, alors que les demandes non authentifiées. Pour plus d'informations sur l'authentification des demandes, consultez Demandes dans la Référence d'API Amazon S3.

Un propriétaire de compartiment peut choisir d'autoriser les demandes non authentifiées. Par exemple, les demandes PutObject non authentifiées sont permises lorsqu'un compartiment dispose d'une politique de compartiment publique ou lorsqu'une ACL de compartiment autorise l'accès `WRITE` ou `FULL_CONTROL` au groupe `All Users` ou spécifiquement à l'utilisateur anonyme. Pour plus d'informations sur les politiques relatives aux compartiments publics et les listes de contrôle d'accès public (ACLs), consultezLa signification du mot « public ».

Toutes les demandes non authentifiées sont faites par l'utilisateur anonyme. Cet utilisateur est représenté ACLs par l'ID `65a011a29cdf8ec533ec3d1ccaae921c` utilisateur canonique spécifique. Si un objet est chargé sur un compartiment via une demande non authentifiée, l'utilisateur anonyme est propriétaire de l'objet. L'ACL d'objet par défaut autorise le `FULL_CONTROL` pour l'utilisateur anonyme en tant que propriétaire de l'objet. Ainsi, Amazon S3 autorise les demandes non authentifiées pour récupérer l'objet ou modifier son ACL.

Pour empêcher les objets d'être modifiés par l'utilisateur anonyme, nous vous recommandons de ne pas mettre en œuvre de politiques de bucket qui autorisent les écritures publiques anonymes dans votre bucket ou d'utiliser des politiques ACLs permettant à l'utilisateur anonyme d'accéder en écriture à votre bucket. Vous pouvez faire appliquer ce comportement recommandé à l'aide du blocage de l'accès public Amazon S3.

Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3. Pour plus d'informations sur ACLs, consultez Présentation de la liste de contrôle d'accès (ACL).

> **Important**
>
> Nous vous recommandons de ne pas utiliser les informations d'identification de l'utilisateur Compte AWS root pour effectuer des demandes authentifiées. Il est préférable de créer un rôle IAM, puis de lui accorder un accès total. Nous appelons les utilisateurs possédant ce rôle des administrateurs. Vous pouvez utiliser les informations d'identification attribuées au rôle d'administrateur, au lieu des informations d'identification de l'utilisateur Compte AWS root, pour interagir avec AWS et effectuer des tâches, telles que créer un bucket, créer des

utilisateurs et accorder des autorisations. Pour plus d'informations, consultez Informations d'identification de sécuritéAWS et Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Politiques de compartiment pour Amazon S3

Une politique de compartiment est une politique basée sur les ressources que vous pouvez utiliser pour accorder des autorisations d'accès à votre compartiment Amazon S3 et aux objets qu'il contient. Seul le propriétaire du compartiment peut associer une politique à un compartiment. Les autorisations attachées au compartiment s'appliquent à tous les objets du compartiment appartenant au compte propriétaire du compartiment. Ces autorisations ne s'appliquent pas aux objets appartenant à d'autres personnes Comptes AWS.

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour contrôler la propriété des objets chargés dans votre compartiment et pour désactiver ou activer les listes de contrôle d'accès ()ACLs. Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket et tous ACLs sont désactivés. Le propriétaire du compartiment détient tous les objets présents dans le compartiment et gère l'accès aux données exclusivement au moyen de politiques.

Les politiques de compartiment utilisent un langage de stratégie basé sur JSON AWS Identity and Access Management (IAM). Vous pouvez utiliser des politiques de compartiment pour ajouter ou refuser des autorisations pour les objets d'un compartiment. Les politiques de compartiment peuvent autoriser ou refuser les requêtes en fonction des éléments de la politique. Ces éléments comprennent le demandeur, les actions S3, les ressources et les aspects ou conditions de la requête (comme l'adresse IP utilisée pour effectuer la requête).

Par exemple, vous pouvez créer une politique de compartiment qui effectue les actions suivantes :

- Accorde à d'autres comptes des autorisations intercompte pour charger des objets dans votre compartiment S3.
- Assurez-vous que vous, le propriétaire du compartiment, avez le contrôle total des objets chargés.

Pour de plus amples informations, veuillez consulter Exemples de politiques de compartiment Amazon S3.

> **Important**
>
> Vous ne pouvez pas utiliser une politique de compartiment pour empêcher les suppressions ou les transitions régies par une règle de cycle de vie S3. Par exemple, même si votre politique de compartiment refuse toutes les actions pour tous les principaux, votre configuration du cycle de vie S3 continue de fonctionner normalement.

Les rubriques de cette section fournissent des exemples et indiquent comment ajouter une politique de compartiment dans la console S3. Pour plus d'informations sur l'utilisation des politiques basées sur l'identité, consultez Politiques basées sur l'identité pour Amazon S3. Pour plus d'informations sur le langage des politiques de compartiment, consultez Politiques, stratégies et autorisations dans Amazon S3.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Rubriques

- Ajout d'une politique de compartiment à l'aide de la console Amazon S3
- Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment
- Exemples de politiques de compartiment Amazon S3
- Exemples de politiques de compartiment utilisant des clés de condition

Ajout d'une politique de compartiment à l'aide de la console Amazon S3

Vous pouvez utiliser le générateur de politiques AWS et la console Amazon S3 pour ajouter une nouvelle politique de compartiment ou modifier une politique de compartiment existante. Une politique de compartiment est une politique basée sur les ressources AWS Identity and Access Management (IAM). Vous ajoutez une politique de compartiment à un compartiment pour accorder à d'autres utilisateurs Comptes AWS ou à des utilisateurs IAM des autorisations d'accès pour le compartiment et les objets qu'il contient. Les autorisations d'objets ne s'appliquent qu'aux objets créés par le propriétaire du compartiment. Pour plus d'informations sur les stratégies de compartiment, consultez Gestion des identités et des accès pour Amazon S3.

Veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions provenant d' AWS Identity and Access Management Access Analyzer avant d'enregistrer

votre stratégie. IAM Access Analyzer exécute des vérifications de politiques pour valider votre politique par rapport à la grammaire de politique et aux bonnes pratiques IAM. Ces vérifications génèrent des résultats et fournissent des recommandations exploitables pour vous aider à créer des stratégies fonctionnelles et conformes aux bonnes pratiques en matière de sécurité. Pour en savoir plus sur la validation des politiques à l'aide d'IAM Access Analyzer, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM. Pour afficher la liste des avertissements, erreurs et suggestions renvoyés par IAM Access Analyzer, consultez la Référence de vérification de politique IAM Access Analyzer.

Pour obtenir des conseils sur la résolution des erreurs liées à une politique, consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3.

Pour créer ou modifier une politique de compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez créer une politique de compartiment ou dont vous souhaitez modifier la politique de compartiment.
4. Sélectionnez l'onglet Autorisations.
5. Sous Politique de compartiment, choisissez Modifier. La page Edit bucket policy (Modifier la politique de compartiment) s'affiche.
6. Dans la page Modifier la stratégie de compartiment, procédez de l'une des manières suivantes :

   - Pour voir des exemples de politiques de compartiment, choisissez Exemples de politiques. Vous pouvez aussi consulter Exemples de politiques de compartiment Amazon S3 dans le Guide de l'utilisateur Amazon S3.
   - Pour générer une politique automatiquement, ou modifier le JSON dans la section Policy (Politique), choisissez Policy generator (Générateur de politique).

   Si vous choisissez le générateur de AWS politiques, celui-ci s'ouvre dans une nouvelle fenêtre.

   a. Sur la page AWS Policy Generator (Générateur de politiques), pour Select Type of Policy (Sélectionner le type de politique), sélectionnez S3 Bucket Policy (Politique de compartiment S3).

b. Ajoutez une instruction en saisissant les informations dans les champs fournis, puis choisissez Add Statement (Ajouter une instruction). Répétez l'opération pour autant d'instructions que vous souhaitez ajouter. Pour plus d'informations sur ces champs, consultez la Référence des éléments de politique IAM JSON dans le Guide de l'utilisateur IAM.

> **Note**
>
> Pour plus de commodité, la page Modifier la stratégie de compartiment affiche l'ARN (Amazon Resource Name) du compartiment actuel au-dessus du champ de texte Stratégie. Vous pouvez copier cet ARN pour l'utiliser dans les instructions de la page AWS Policy Generator (Générateur de politique).

c. Une fois que vous avez fini d'ajouter des instructions, choisissez Generate Policy (Générer une stratégie).

d. Copiez le texte de stratégie généré, choisissez Fermer et revenez à la page Modifier la stratégie de compartiment dans la console Amazon S3.

7. Dans la zone Politique, modifiez la politique existante ou collez la politique de compartiment depuis le générateur de AWS politiques. Veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions avant d'enregistrer votre stratégie.

> **Note**
>
> Les politiques de compartiment sont limitées à une taille de 20 Ko.

8. (Facultatif) Choisissez Preview external access (Aperçu de l'accès externe) dans le coin inférieur droit pour avoir un aperçu de la façon dont votre nouvelle politique affecte l'accès public et l'accès intercompte à votre ressource. Avant d'enregistrer votre stratégie, vous pouvez vérifier si elle introduit de nouveaux résultats IAM Access Analyzer ou si elle résout les résultats existants. Si vous ne voyez pas d'analyseur actif, choisissez Go to Access Analyzer (Accédez à l'analyseur d'accès) pour créer un analyseur de compte dans l'analyseur d'accès IAM. Pour plus d'informations, consultez Prévisualisation des accès dans le Guide de l'utilisateur IAM.

9. Choisissez Save changes (Enregistrer les modifications), ce qui vous ramène à l'onglet Permissions (Autorisations).

Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment

Vous pouvez utiliser les politiques relatives aux compartiments Amazon S3 pour contrôler l'accès aux compartiments à partir de points de terminaison de cloud privé virtuel (VPC) spécifiques ou spécifiques. VPCs Cette section contient des exemples de politiques de compartiment qui peuvent être utilisés pour contrôler l'accès aux compartiments Amazon S3 à partir des points de terminaison d'un VPC. Pour apprendre à configurer les points de terminaison d'un VPC, consultez Points de terminaison d'un VPC dans le Guide de l'utilisateur VPC.

Un VPC vous permet de lancer des AWS ressources dans un réseau virtuel que vous définissez. Le point de terminaison d'un VPC vous permet de créer une connexion privée entre votre VPC et un autre Service AWS. Cette connexion privée ne nécessite pas d'accès via Internet, via une connexion de réseau privé virtuel (VPN), via une instance NAT ou via AWS Direct Connect.

Le point de terminaison d'un VPC pour Amazon S3 est une entité logique au sein d'un VPC qui permet uniquement une connexion à Amazon S3. Le point de terminaison d'un VPC achemine les demandes vers Amazon S3 et les réponses renvoyées au VPC. Les points de terminaison d'un VPC changent uniquement la manière dont les demandes sont acheminées. Les points de terminaison publics Amazon S3 et les noms DNS continuent de fonctionner avec les points de terminaison d'un VPC. Pour obtenir des informations importantes concernant l'utilisation des points de terminaison d'un VPC avec Amazon S3, consultez Points de terminaison de passerelle et Points de terminaison de passerelle pour Amazon S3 dans le Guide de l'utilisateur VPC.

Les points de terminaison d'un VPC pour Amazon S3 offrent deux façons de contrôler l'accès à vos données Amazon S3 :

- Vous pouvez contrôler les demandes, les utilisateurs ou les groupes autorisés à traverser un point de terminaison d'un VPC spécifique. Pour plus d'informations sur ce type de contrôle d'accès, consultez Contrôle de l'accès aux points de terminaison d'un VPC à l'aide de politiques de point de terminaison dans le Guide de l'utilisateur VPC.
- Vous pouvez contrôler quels points de terminaison VPCs ou quels points de terminaison VPC ont accès à vos compartiments en utilisant les politiques relatives aux compartiments Amazon S3. Pour obtenir des exemples de ce type de contrôle d'accès avec politique de compartiment, consultez les rubriques suivantes sur les restrictions d'accès.

Rubriques

- Restriction de l'accès à un point de terminaison d'un VPC spécifique

- Restriction de l'accès à un VPC spécifique

> **Important**
>
> Lors de l'application de politiques de compartiment Amazon S3 pour les points de terminaison d'un VPC décrits dans cette section, vous pouvez bloquer involontairement l'accès au compartiment. Les autorisations attribuées à un compartiment dans le but de restreindre l'accès aux connexions issues du point de terminaison de votre VPC peuvent bloquer toutes les connexions à ce compartiment. Pour plus d'informations sur la résolution de ce problème, consultez Comment corriger ma politique de compartiment lorsqu'elle a le mauvais VPC ou le mauvais ID de point de terminaison du VPC ? dans le Centre de connaissances AWS Support .

Restriction de l'accès à un point de terminaison d'un VPC spécifique

Voici un exemple de politique de compartiment Amazon S3 qui restreint l'accès à un compartiment spécifique, `awsexamplebucket1`, uniquement à partir du point de terminaison d'un VPC doté de l'ID `vpce-1a2b3c4d`. Si le point de terminaison spécifié n'est pas utilisé, la politique refuse tout accès au compartiment. La condition `aws:SourceVpce` spécifie le point de terminaison. La condition `aws:SourceVpce` ne requiert pas d'Amazon Resource Name (ARN) pour la ressource du point de terminaison de VPC, uniquement l'ID de point de terminaison du VPC. Pour plus d'informations sur l'utilisation de conditions dans une stratégie, consultez Exemples de politiques de compartiment utilisant des clés de condition.

> **Important**
>
> - Avant d'utiliser l'exemple de stratégie suivant, remplacez l'ID de point de terminaison du VPC par une valeur appropriée pour votre cas d'utilisation. Dans le cas contraire, vous ne parviendrez pas à accéder à votre compartiment.
> - Cette politique désactive l'accès de la console au compartiment spécifié, car les demandes de la console ne proviennent pas du point de terminaison du VPC défini.

JSON

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909152",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPCE-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpce": "vpce-1a2b3c4d"
         }
       }
     }
   ]
}
```

Restriction de l'accès à un VPC spécifique

Vous pouvez créer une politique de compartiment qui restreint l'accès à un VPC spécifique en utilisant la condition `aws:SourceVpc`. Ceci est utile si vous avez plusieurs points de terminaison d'un VPC configurés pour le même VPC et que vous voulez gérer l'accès à vos compartiments Amazon S3 pour tous vos points de terminaison. Voici un exemple de politique qui refuse l'accès à `awsexamplebucket1` et ses objets à toute personne extérieure au VPC `vpc-111bbb22`. Si le VPC spécifié n'est pas utilisé, la politique refuse tout accès au compartiment. Cette instruction n'accorde pas l'accès au compartiment. Pour autoriser l'accès, vous devez ajouter une instruction `Allow` séparée. La clé de condition `vpc-111bbb22` ne requiert pas d'ARN pour la ressource VPC, uniquement l'ID du VPC.

> **Important**
>
> - Avant d'utiliser l'exemple de stratégie suivant, remplacez l'ID du VPC par une valeur appropriée pour votre cas d'utilisation. Dans le cas contraire, vous ne parviendrez pas à accéder à votre compartiment.

- Cette politique désactive l'accès de la console au compartiment spécifié, car les demandes de la console ne proviennent pas du VPC défini.

JSON

```
{
   "Version": "2012-10-17",
   "Id": "Policy1415115909153",
   "Statement": [
     {
       "Sid": "Access-to-specific-VPC-only",
       "Principal": "*",
       "Action": "s3:*",
       "Effect": "Deny",
       "Resource": ["arn:aws:s3:::awsexamplebucket1",
                    "arn:aws:s3:::awsexamplebucket1/*"],
       "Condition": {
         "StringNotEquals": {
           "aws:SourceVpc": "vpc-111bbb22"
         }
       }
     }
   ]
}
```

Pour plus d'informations sur la façon de restreindre l'accès à votre compartiment en fonction d'une IPs ou plusieurs adresses IP spécifiques VPCs, consultez Comment autoriser uniquement des points de terminaison ou des adresses IP VPC spécifiques à accéder à mon compartiment Amazon S3 ? dans le AWS re:Post Knowledge Center.

Exemples de politiques de compartiment Amazon S3

Grâce aux politiques de compartiment d'Amazon S3, vous pouvez sécuriser l'accès aux objets de vos compartiments, afin que seuls les utilisateurs disposant des autorisations appropriées puissent y accéder. Vous pouvez même empêcher les utilisateurs authentifiés ne disposant pas des autorisations appropriées d'accéder à vos ressources Amazon S3.

Cette section présente des exemples de cas d'utilisation standard de politiques de compartiment. Ces exemples de politiques utilisent *amzn-s3-demo-bucket* comme valeur de ressource. Pour tester ces politiques, remplacez *user input placeholders* par vos propres informations (comme le nom de votre compartiment).

Pour accorder ou refuser des autorisations à un ensemble d'objets, vous pouvez utiliser des caractères génériques (*) dans Amazon Resource Names (ARNs) et d'autres valeurs. Par exemple, vous pouvez contrôler l'accès aux groupes d'objets qui commencent par un préfixe courant ou se terminent par une extension spécifique, comme `.html`.

Pour plus d'informations sur le langage de politique AWS Identity and Access Management (IAM), consultezPolitiques, stratégies et autorisations dans Amazon S3.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

> **Note**
>
> Lors du test des autorisations à l'aide de la console Amazon S3, vous devez accorder les autorisations supplémentaires requises par la console (`s3:ListAllMyBuckets`, `s3:GetBucketLocation` et `s3:ListBucket`). Pour obtenir un exemple de guide étape par étape pour accorder des autorisations aux utilisateurs et tester ces autorisations à l'aide de la console, consultez Contrôle de l'accès à un compartiment avec des stratégies d'utilisateur.

Voici des ressources supplémentaires pour créer des politiques de compartiment :

- Pour obtenir la liste des actions, des ressources et des clés de condition de politique IAM que vous pouvez utiliser lors de la création d'une politique de compartiment, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.
- Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.
- Pour obtenir des conseils sur la création de votre politique S3, consultez Ajout d'une politique de compartiment à l'aide de la console Amazon S3.
- Pour résoudre les erreurs liées à une politique, consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3.

Si vous ne parvenez pas à ajouter ou à mettre à jour une politique, consultez Pourquoi l'erreur « Principal non valide dans la politique » s'affiche-t-elle lorsque j'essaie de mettre à jour la politique de mon compartiment Amazon S3 ? dans le AWS re:Post Knowledge Center.

Rubriques

- Octroi d'une autorisation en lecture seule à un utilisateur anonyme public
- Obligation de chiffrement
- Gestion des seaux à l'aide de boîtes en conserve ACLs
- Gestion de l'accès aux objets avec l'étiquetage des objets
- Gestion de l'accès aux objets par l'utilisation de clés de condition globales
- Gestion des accès en fonction des requêtes HTTP ou HTTPS
- Gestion de l'accès des utilisateurs à des dossiers spécifiques
- Gestion des accès pour les journaux d'accès
- Gérer l'accès à un Amazon CloudFront OAI
- Gestion des accès pour Amazon S3 Storage Lens
- Gestion des autorisations pour l'inventaire S3, les analyses S3 et les rapports d'inventaire S3
- Exigence d'une MFA
- Empêcher les utilisateurs de supprimer des objets

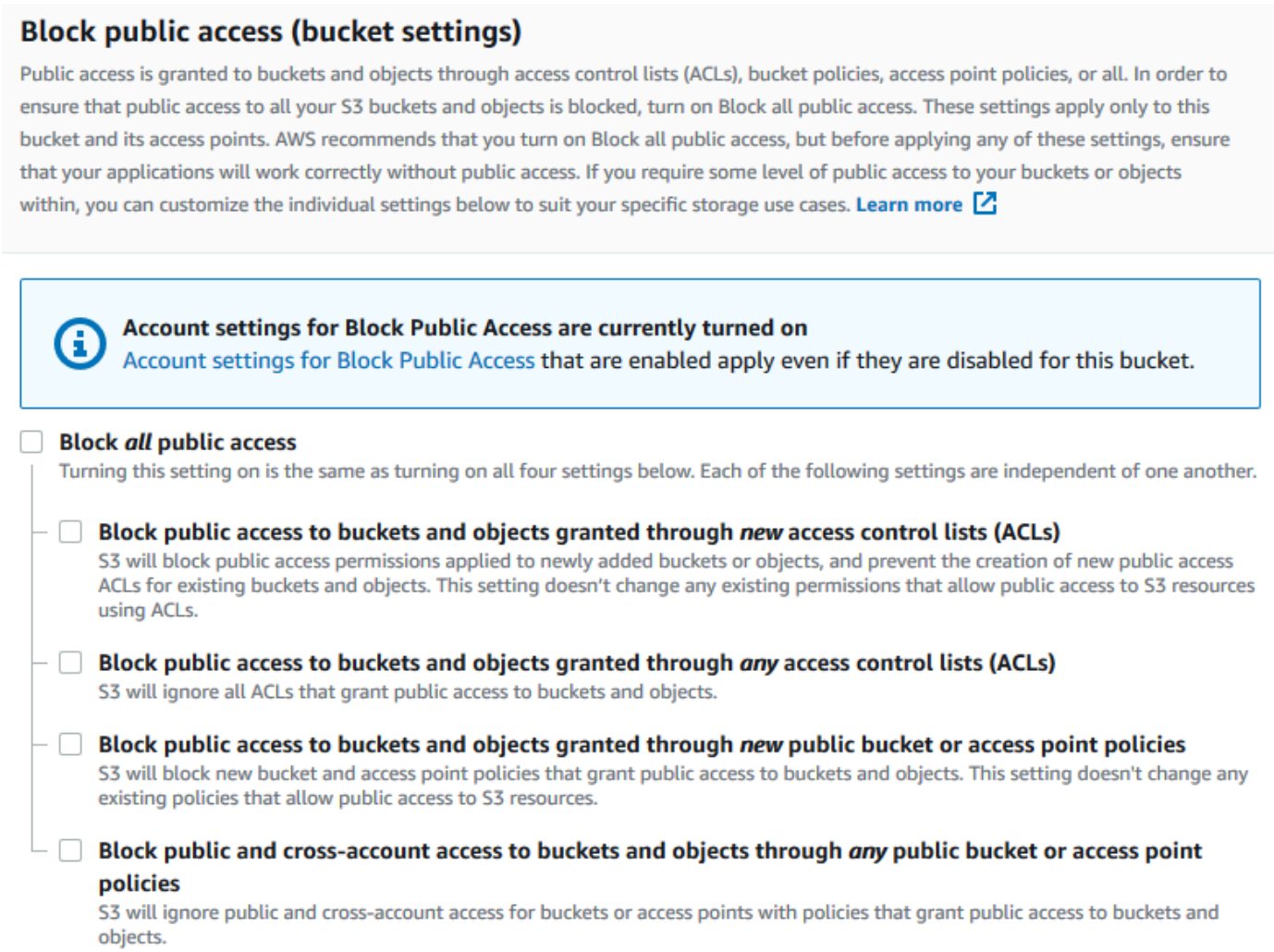
Octroi d'une autorisation en lecture seule à un utilisateur anonyme public

Vous pouvez utiliser vos paramètres de politique pour accorder l'accès à des utilisateurs anonymes publics, ce qui est utile si vous configurez votre compartiment en tant que site web statique. Pour accorder l'accès à des utilisateurs anonymes publics, vous devez désactiver les paramètres de blocage de l'accès public pour votre compartiment. Pour plus d'informations sur la marche à suivre et sur la politique requise, consultez Définition des autorisations pour l'accès au site web. Pour savoir comment configurer des politiques plus restrictives dans le même but, consultez Comment accorder un accès public en lecture à certains objets de mon compartiment Amazon S3 ? dans le AWS Knowledge Center.

Par défaut, Amazon S3 bloque l'accès public à votre compte et à vos compartiments. Si vous souhaitez utiliser un compartiment pour héberger un site web statique, vous pouvez utiliser ces étapes pour modifier vos paramètres de blocage de l'accès public.

> **Warning**
>
> Avant de suivre ces étapes, passez en revue Blocage de l'accès public à votre stockage Amazon S3 pour vous assurer que vous comprenez et acceptez les risques liés à l'autorisation de l'accès public. Lorsque vous désactivez les paramètres de blocage de l'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tous les accès publics à vos compartiments.

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le nom du compartiment que vous avez configuré en tant que site web statique.
3. Choisissez Permissions.
4. Sous Block public access (bucket settings) (Bloquer l'accès public (paramètres de compartiment)), choisissez Edit (Modifier).
5. Décochez Bloquer tous les accès publics et sélectionnez Enregistrer les modifications.



Amazon S3 désactive les paramètres de blocage de l'accès public pour votre compartiment. Pour créer un site Web public statique, vous devrez peut-être aussi modifier les paramètres de blocage de l'accès public de votre compte avant d'ajouter une politique de compartiment. Si les paramètres de blocage de l'accès public pour votre compte sont actuellement activés, une note s'affiche sous Bloquer l'accès public (paramètres de compartiment).

Obligation de chiffrement

Vous pouvez exiger un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), comme indiqué dans les exemples suivants.

Exiger le SSE-KMS pour tous les objets enregistrés dans un compartiment

L'exemple de politique suivant exige que chaque objet écrit dans le compartiment soit chiffré avec un chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Si l'objet n'est pas chiffré avec SSE-KMS, la demande sera refusée.

JSON

```
{
"Version": "2012-10-17",
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMS",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "Null": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "true"
    }
  }
}]
}
```

Exiger un SSE-KMS avec un AWS KMS key spécifique pour tous les objets enregistrés dans un compartiment

L'exemple de politique suivant interdit l'écriture d'objets dans le compartiment s'ils ne sont pas chiffrés avec SSE-KMS en utilisant un ID de clé KMS spécifique. Même si les objets sont chiffrés avec SSE-KMS en utilisant un en-tête par demande ou le chiffrement par défaut des compartiments, les objets ne peuvent pas être écrits dans le compartiment s'ils n'ont pas été chiffrés avec la clé KMS spécifiée. Assurez-vous de remplacer la clé KMS ARN utilisée dans cet exemple par votre propre clé KMS ARN.

JSON

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

```
"Id": "PutObjPolicy",
"Statement": [{
  "Sid": "DenyObjectsThatAreNotSSEKMSWithSpecificKey",
  "Principal": "*",
  "Effect": "Deny",
  "Action": "s3:PutObject",
  "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
  "Condition": {
    "ArnNotEqualsIfExists": {
      "s3:x-amz-server-side-encryption-aws-kms-key-id": "arn:aws:kms:us-
east-2:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"
    }
  }
}]
}
```

Gestion des seaux à l'aide de boîtes en conserve ACLs

Octroi d'autorisations à plusieurs comptes pour télécharger des objets ou définir un objet ACLs pour un accès public

L'exemple de politique utilisateur suivant octroie les autorisations `s3:PutObject` et `s3:PutObjectAcl` à plusieurs Comptes AWS. De plus, cet exemple de politique exige que toute demande correspondant à ces opérations inclue la liste ACL prédéfinie `public-read`. Pour plus d'informations, consultez Actions de politique pour Amazon S3 et Clés de condition de politique pour Amazon S3.

> **Warning**
>
> L'ACL prédéfinie `public-read` permet à n'importe qui dans le monde entier de visualiser les objets de votre compartiment. Soyez vigilant lors de l'octroi de l'accès anonyme à votre compartiment Amazon S3 ou de la désactivation des paramètres du blocage de l'accès public. Lorsque vous accordez un accès anonyme, tout le monde peut accéder à votre compartiment. Il est recommandé de ne jamais autoriser un accès anonyme à votre compartiment Amazon S3 à moins que vous n'en ayez spécifiquement besoin, comme dans le cas de l'hébergement de site web statique. Si vous souhaitez activer les paramètres de blocage de l'accès public pour l'hébergement de sites Web statiques, consultez Tutoriel : configuration d'un site web statique sur Amazon S3.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AddPublicReadCannedAcl",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::444455556666:root"
                ]
            },
            "Action": [
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": [
                        "public-read"
                    ]
                }
            }
        }
    ]
}
```

Octroi d'autorisations intercomptes pour charger des objets tout en garantissant que le propriétaire du compartiment dispose d'un contrôle total

L'exemple suivant montre comment autoriser une autre personne Compte AWS à télécharger des objets dans votre compartiment tout en vous assurant que vous avez le contrôle total des objets chargés. Cette politique accorde à un compte spécifique Compte AWS (*111122223333*) la possibilité de télécharger des objets uniquement si ce compte inclut l'ACL `bucket-owner-full-control` prédéfinie lors du téléchargement. La condition `StringEquals` figurant dans la politique spécifie la clé de la condition `s3:x-amz-acl` pour exprimer l'exigence de l'ACL prédéfinie. Pour de plus amples informations, veuillez consulter Clés de condition de politique pour Amazon S3.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
     {
       "Sid":"PolicyForAllowUploadWithACL",
       "Effect":"Allow",
       "Principal":{"AWS":"111122223333"},
       "Action":"s3:PutObject",
       "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
       "Condition": {
         "StringEquals": {"s3:x-amz-acl":"bucket-owner-full-control"}
       }
     }
   ]
}
```

Gestion de l'accès aux objets avec l'étiquetage des objets

Autoriser un utilisateur à lire uniquement les objets qui ont une clé et une valeur d'étiquette spécifiques

La politique d'autorisations suivante limite un utilisateur à la seule lecture des objets qui comportent la clé et la valeur d'étiquette `environment: production`. Cette politique utilise la clé de condition `s3:ExistingObjectTag` pour spécifier la clé et la valeur d'étiquette.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Principal":{
            "AWS":"arn:aws:iam::111122223333:role/JohnDoe"
         },
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
```

```
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringEquals":{
               "s3:ExistingObjectTag/environment":"production"
            }
         }
      }
   ]
}
```

Restreindre les clés d'étiquette d'objet que les utilisateurs peuvent ajouter

L'exemple de politique suivant accorde à un utilisateur l'autorisation d'exécuter l'action `s3:PutObjectTagging`, qui permet à un utilisateur d'ajouter des étiquettes à un objet existant. La condition utilise la clé de condition `s3:RequestObjectTagKeys` pour spécifier les clés d'étiquette autorisées, telles que `Owner` ou `CreationDate`. Pour plus d'informations, consultez Création d'une condition avec plusieurs clés ou valeurs dans le Guide de l'utilisateur IAM.

Cette politique garantit que chaque clé d'étiquette spécifiée dans la demande est une clé d'étiquette autorisée. Le qualificateur `ForAnyValue` dans la condition garantit qu'au moins une des clés spécifiées doit être présente dans la demande.

JSON

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
            "arn:aws:iam::111122223333:role/JohnDoe"
         ]
       },
 "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"ForAnyValue:StringEquals": {"s3:RequestObjectTagKeys": [
            "Owner",
```

```
            "CreationDate"
          ]
        }
      }
    }
  ]
}
```

Exiger une clé et une valeur d'étiquette spécifiques pour permettre aux utilisateurs d'ajouter des étiquettes d'objet

L'exemple de politique suivant accorde à un utilisateur l'autorisation d'exécuter l'action `s3:PutObjectTagging`, qui permet à un utilisateur d'ajouter des étiquettes à un objet existant. La condition exige que l'utilisateur inclue une clé d'étiquette spécifique (telle que *`Project`*) avec la valeur définie sur *`X`*.

JSON

```
{
   "Version": "2012-10-17",
  "Statement": [
    {"Principal":{"AWS":[
       "arn:aws:iam::111122223333:user/JohnDoe"
         ]
       },
      "Effect": "Allow",
      "Action": [
        "s3:PutObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {"StringEquals": {"s3:RequestObjectTag/Project": "X"
        }
      }
    }
  ]
}
```

Permettre à un utilisateur de n'ajouter que des objets ayant une clé et une valeur d'étiquetage d'objet spécifiques

L'exemple de politique suivant accorde à un utilisateur l'autorisation d'effectuer l'action `s3:PutObject` afin qu'il puisse ajouter des objets à un compartiment. Cependant, l'instruction `Condition` restreint les clés et les valeurs d'étiquetage qui sont autorisées sur les objets chargés. Dans cet exemple, l'utilisateur ne peut ajouter au compartiment que les objets ayant la clé d'étiquette spécifique (*`Department`*) avec la valeur définie sur *`Finance`*.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Principal":{
            "AWS":[
                 "arn:aws:iam::111122223333:user/JohnDoe"
         ]
        },
        "Effect": "Allow",
        "Action": [
            "s3:PutObject"
        ],
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket/*"
        ],
        "Condition": {
            "StringEquals": {
                "s3:RequestObjectTag/Department": "Finance"
            }
        }
    }]
}
```

Gestion de l'accès aux objets par l'utilisation de clés de condition globales

Les clés de condition globales sont des clés de contexte de condition avec un `aws` préfixe. Services AWS peut prendre en charge les clés de condition globales ou les clés spécifiques au service qui incluent le préfixe du service. Vous pouvez utiliser l'élément `Condition` d'une politique JSON pour comparer les clés d'une requête avec les valeurs des clés que vous spécifiez dans votre politique.

Restreindre l'accès aux seules livraisons du journal d'accès du serveur Amazon S3

Dans l'exemple de politique de compartiment suivant, la clé de condition aws:SourceArnglobale est utilisée pour comparer le nom de ressource Amazon (ARN) de la ressource, en effectuant une service-to-service demande avec l'ARN spécifié dans la politique. La clé de condition globale `aws:SourceArn` est utilisée pour empêcher le service Amazon S3 d'être utilisé comme adjoint confus lors de transactions entre services. Seul le service Amazon S3 est autorisé à ajouter des objets au compartiment Amazon S3.

Cet exemple de stratégie de compartiment accorde uniquement des autorisations `s3:PutObject` au principal du service de journalisation (`logging.s3.amazonaws.com`).

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowPutObjectS3ServerAccessLogsPolicy",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111111111111"
                },
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::EXAMPLE-SOURCE-BUCKET"
                }
            }
        },
        {
            "Sid": "RestrictToS3ServerAccessLogs",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket-logs/*",
            "Condition": {
                "ForAllValues:StringNotEquals": {
```

```
                    "aws:PrincipalServiceNamesList": "logging.s3.amazonaws.com"
                }
            }
        }
    ]
}
```

Autoriser l'accès uniquement à votre organisation

Si vous souhaitez que tous les principaux IAM accédant à une ressource proviennent d'un Compte AWS compte de gestion (y compris le compte de AWS Organizations gestion), vous pouvez utiliser la clé de condition globale `aws:PrincipalOrgID`.

Pour accorder ou restreindre ce type d'accès, définissez la condition `aws:PrincipalOrgID` et définissez la valeur de l'ID de votre organisation dans la politique de compartiment. L'ID de l'organisation permet de contrôler l'accès au compartiment. Lorsque vous utilisez la condition `aws:PrincipalOrgID`, les autorisations de la politique de compartiment sont également appliquées à tous les nouveaux comptes qui sont ajoutés à l'organisation.

Voici un exemple de politique de compartiment basée sur les ressources que vous pouvez utiliser pour accorder à des principaux IAM spécifiques de votre organisation un accès direct à votre compartiment. En ajoutant la clé de condition globale `aws:PrincipalOrgID` à votre politique de compartiment, le compte principal doit désormais faire partie de votre organisation pour obtenir l'accès à la ressource. Même si vous spécifiez accidentellement un compte incorrect lors de l'octroi de l'accès, la clé de condition globale aws:PrincipalOrgID constitue une protection supplémentaire. Lorsque cette clé globale est utilisée dans une politique, elle empêche tous les principaux de l'extérieur de l'organisation spécifiée d'accéder au compartiment S3. Seuls les principaux des comptes de l'organisation listée peuvent obtenir l'accès à la ressource.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "AllowGetObject",
        "Principal": {
            "AWS": "*"
        },
        "Effect": "Allow",
```

```
        "Action": "s3:GetObject",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
        "Condition": {
            "StringEquals": {
                "aws:PrincipalOrgID": ["o-aa111bb222"]
            }
        }
    }]
}
```

Gestion des accès en fonction des requêtes HTTP ou HTTPS

Restreindre l'accès aux seules requêtes HTTPS

Si vous voulez empêcher les attaquants potentiels de manipuler le trafic réseau, vous pouvez utiliser HTTPS (TLS) pour n'autoriser que les connexions chiffrées tout en limitant l'accès à votre compartiment aux requêtes HTTP. Pour déterminer si la requête est HTTP ou HTTPS, utilisez la clé de condition globale aws:SecureTransport dans votre politique de compartiment S3. La clé de condition `aws:SecureTransport` vérifie si une requête a été envoyée en utilisant HTTP.

Si une demande renvoie `true`, alors la demande a été envoyée par HTTPS. Si une demande renvoie `false`, alors la demande a été envoyée par HTTP. Vous pouvez ensuite autoriser ou refuser l'accès à votre compartiment en fonction du schéma de requête souhaité.

Dans l'exemple suivant, la politique de compartiment refuse explicitement les demandes HTTP.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [{
        "Sid": "RestrictToTLSRequestsOnly",
        "Action": "s3:*",
        "Effect": "Deny",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket",
            "arn:aws:s3:::example-s3-bucket;/*"
        ],
        "Condition": {
            "Bool": {
```

```
                "aws:SecureTransport": "false"
            }
        },
        "Principal": "*"
    }]
}
```

Restreindre l'accès à un référent HTTP spécifique

Supposons que vous ayez un site web avec le nom de domaine *www.example.com* ou *example.com*, avec des liens vers des photos et des vidéos stockées dans votre compartiment nommé *amzn-s3-demo-bucket*. Par défaut, toutes les ressources Amazon S3 sont privées, de sorte que seul Compte AWS celui qui les a créées peut y accéder.

Pour autoriser l'accès en lecture à ces objets à partir de votre site Web, vous pouvez ajouter une politique de compartiment qui accorde l'autorisation `s3:GetObject` avec une condition stipulant que la requête GET provienne initialement de pages Web spécifiques. La politique suivante limite les requêtes en utilisant la condition `StringLike` avec la clé de condition `aws:Referer`.

JSON

```
{
  "Version":"2012-10-17",
  "Id":"HTTP referer policy example",
  "Statement":[
    {
      "Sid":"Allow only GET requests originating from www.example.com and
 example.com.",
      "Effect":"Allow",
      "Principal":"*",
      "Action":["s3:GetObject","s3:GetObjectVersion"],
      "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition":{
        "StringLike":{"aws:Referer":["http://www.example.com/*","http://
example.com/*"]}
      }
    }
  ]
}
```

Veillez à ce que les navigateurs que vous utilisez incluent l'en-tête HTTP `referer` dans la demande.

> **Warning**
>
> Nous vous recommandons de faire preuve de prudence lorsque vous utilisez la clé de condition `aws:Referer`. Il est dangereux d'inclure une valeur d'en-tête de référent HTTP connu publiquement. Les tiers non autorisés peuvent utiliser des navigateurs modifiés ou personnalisés pour fournir n'importe quelle valeur `aws:Referer` de leur choix. Par conséquent, ne l'utilisez pas `aws:Referer` pour empêcher des parties non autorisées de faire des AWS demandes directes.
>
> La clé de condition `aws:Referer` est fournie uniquement pour permettre aux clients de protéger leur contenu numérique, stocké notamment dans Simple Storage Service (Amazon S3), contre tout référencement sur des sites tiers non autorisés. Pour plus d'informations, consultez aws:Referer dans le Guide de l'utilisateur IAM.

Gestion de l'accès des utilisateurs à des dossiers spécifiques

Accorder aux utilisateurs l'accès à des dossiers spécifiques

Supposons que vous essayez d'accorder aux utilisateurs l'accès à un dossier spécifique. Si l'utilisateur IAM et le compartiment S3 appartiennent à la même entité Compte AWS, vous pouvez utiliser une politique IAM pour accorder à l'utilisateur l'accès à un dossier de compartiment spécifique. Avec cette approche, vous n'avez pas besoin de mettre à jour votre politique de compartiment pour octroyer l'accès. Vous pouvez ajouter la politique IAM à un rôle IAM auquel plusieurs utilisateurs peuvent basculer.

Si l'identité IAM et le compartiment S3 appartiennent à des entités différentes Comptes AWS, vous devez accorder un accès entre comptes à la fois dans la politique IAM et dans la politique de compartiment. Pour plus d'informations sur l'octroi d'un accès intercompte, consultez Bucket owner granting cross-account bucket permissions (Propriétaire du compartiment accordant des autorisations intercomptes pour le compartiment).

L'exemple suivant de politique de compartiment accorde à *JohnDoe* un accès complet à la console à son seul dossier (`home/JohnDoe/`). En créant un dossier `home` et en accordant les autorisations appropriées à vos utilisateurs, vous pouvez faire en sorte que plusieurs utilisateurs partagent un seul compartiment. Cette politique se compose de trois instructions `Allow` :

- *AllowRootAndHomeListingOfCompanyBucket* : permet à l'utilisateur (*JohnDoe*) de lister les objets au niveau de la racine du compartiment *amzn-s3-demo-bucket* et dans le dossier home. Cette instruction permet également à l'utilisateur d'effectuer une recherche sur le préfixe home/ en utilisant la console.
- *AllowListingOfUserFolder* : permet à l'utilisateur (*JohnDoe*) de lister tous les objets du dossier home/*JohnDoe*/ et de ses sous-dossiers éventuels.
- *AllowAllS3ActionsInUserFolder* : permet à l'utilisateur d'effectuer toutes les actions Amazon S3 en accordant des autorisations `Read`, `Write` et `Delete`. Les autorisations sont limitées au dossier personnel du propriétaire du compartiment.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowRootAndHomeListingOfCompanyBucket",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringEquals": {
                    "s3:prefix": ["", "home/", "home/JohnDoe"],
                    "s3:delimiter": ["/"]
                }
            }
        },
        {
            "Sid": "AllowListingOfUserFolder",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:ListBucket"],
```

```
            "Effect": "Allow",
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket"],
            "Condition": {
                "StringLike": {
                    "s3:prefix": ["home/JohnDoe/*"]
                }
            }
        },
        {
            "Sid": "AllowAllS3ActionsInUserFolder",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/JohnDoe"
                ]
            },
            "Action": ["s3:*"],
            "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket/home/JohnDoe/*"]
        }
    ]
}
```

Gestion des accès pour les journaux d'accès

Accorder l'accès à l'Application Load Balancer pour activer les journaux d'accès

Lorsque vous activez les journaux d'accès pour Application Load Balancer, vous devez spécifier le nom du compartiment S3 où l'équilibreur de charge stockera les journaux. Le compartiment doit comporter une politique attachée qui accorde à Elastic Load Balancing l'autorisation d'écrire dans le compartiment.

Dans l'exemple suivant, la politique de compartiment accorde à Elastic Load Balancing (ELB) l'autorisation d'écrire les journaux d'accès dans le compartiment :

JSON

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

```
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/
AWSLogs/111122223333/*"
        }
    ]
}
```

> **Note**
>
> Assurez-vous de remplacer *elb-account-id* par l'ID du Compte AWS d'Elastic Load Balancing pour votre Région AWS. Pour obtenir la liste des régions Elastic Load Balancing, consultez Attach a policy to your Amazon S3 bucket (Association d'une politique à votre compartiment Amazon S3) dans le Guide de l'utilisateur Elastic Load Balancing.

Si vous Région AWS ne figurez pas dans la liste des régions Elastic Load Balancing prises en charge, appliquez la politique suivante, qui accorde des autorisations au service de livraison de journaux spécifié.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
       "Principal": {
         "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
          },
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/prefix/AWSLogs/111122223333/
*"
    }
  ]
}
```

Ensuite, veillez à configurer vos journaux d'accès Elastic Load Balancing en les activant. Vous pouvez vérifier les autorisations de votre compartiment en créant un fichier de test.

Gérer l'accès à un Amazon CloudFront OAI

Accorder une autorisation à un Amazon CloudFront OAI

L'exemple de politique de compartiment suivant accorde à une identité CloudFront d'accès d'origine (OAI) l'autorisation d'obtenir (lire) tous les objets de votre compartiment S3. Vous pouvez utiliser un CloudFront OAI pour autoriser les utilisateurs à accéder aux objets de votre compartiment via Amazon S3 CloudFront , mais pas directement. Pour plus d'informations, consultez Restreindre l'accès au contenu Amazon S3 à l'aide d'une identité d'accès d'origine dans le manuel Amazon CloudFront Developer Guide.

La stratégie suivante utilise l'ID de l'OAI comme stratégie de `Principal`. Pour plus d'informations sur l'utilisation des politiques de compartiment S3 pour accorder l'accès à un CloudFront OAI, consultez la section Migration de l'identité d'accès d'origine (OAI) vers le contrôle d'accès d'origine (OAC) dans le manuel Amazon Developer Guide. CloudFront

Pour utiliser cet exemple :

- Remplacez *EH1HDMB1FH2TC* par l'ID OAI. Pour trouver l'ID de l'OAI, consultez la page Origin Access Identity sur la CloudFront console ou utilisez-le ListCloudFrontOriginAccessIdentitiesdans l' CloudFront API.
- Remplacez *amzn-s3-demo-bucket* par le nom de votre compartiment.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
```

```
        }
    ]
}
```

Gestion des accès pour Amazon S3 Storage Lens

Accorder des autorisations pour Amazon S3 Storage Lens

S3 Storage Lens regroupe vos métriques et affiche les informations dans la section Instantané du compte sur la page Compartiments de la console Amazon S3. S3 Storage Lens fournit également un tableau de bord interactif que vous pouvez utiliser pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord dispose d'options d'exploration pour générer et visualiser des informations au niveau de l'organisation, du compte, de la Région AWS, de la classe de stockage, du compartiment, du préfixe ou du groupe Storage Lens. Vous pouvez également envoyer une exportation de métriques quotidienne au format CSV ou Parquet vers un compartiment S3.

S3 Storage Lens peut exporter vos métriques d'utilisation du stockage agrégées vers un compartiment Amazon S3 pour une analyse plus approfondie. Le compartiment dans lequel S3 Storage Lens place ses exportations de métriques porte le nom de compartiment de destination. Lorsque vous configurez l'exportation des métriques S3 Storage Lens, vous devez disposer d'une politique de compartiment pour le compartiment de destination. Pour plus d'informations, consultez Évaluer l'activité et l'utilisation de votre stockage avec Amazon S3 Storage Lens.

L'exemple de politique de compartiment suivant octroie à Amazon S3 l'autorisation d'écrire des objets (requêtes PUT) dans un compartiment de destination. Vous utilisez une politique de compartiment comme celle-ci sur le compartiment de destination lorsque vous configurez les mesures de S3 Storage Lens.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3StorageLensExamplePolicy",
            "Effect": "Allow",
            "Principal": {
```

```
                "Service": "storage-lens.s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/111122223333/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control",
                    "aws:SourceAccount": "111122223333",
                    "aws:SourceArn": "arn:aws:s3:region-
code:111122223333:storage-lens/storage-lens-dashboard-configuration-id"
                }
            }
        }
    ]
}
```

Lorsque vous configurez une exportation de métriques au niveau de l'organisation S3 Storage Lens, utilisez la modification suivante de l'instruction `Resource` de la politique de compartiment précédente.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/destination-prefix/
StorageLens/your-organization-id/*",
```

Gestion des autorisations pour l'inventaire S3, les analyses S3 et les rapports d'inventaire S3

Accorder des autorisations pour l'inventaire S3 et les analyses S3.

L'inventaire S3 crée des listes d'objets dans un compartiment, et l'exportation de l'analyse de classe de stockage des analyses S3 crée des fichiers de sortie des données utilisées dans l'analyse. Le compartiment pour lequel l'inventaire répertorie les objets est appelé compartiment source. Le compartiment dans lequel le fichier d'inventaire ou le fichier d'exportation analytique est écrit est appelé compartiment de destination. Lorsque vous configurez un inventaire ou une exportation analytique, vous devez créer une politique de compartiment pour le compartiment de destination. Pour plus d'informations, consultez Catalogage et analyse de vos données avec l'inventaire S3 et Analyses Amazon S3 - Analyse de classe de stockage.

L'exemple de politique de compartiment suivant accorde à Amazon S3 l'autorisation d'écrire des objets (requêtes PUT) à partir du compte pour le compartiment source vers le compartiment de destination. Vous utilisez une politique de compartiment comme celle-ci sur le compartiment de destination lors de la configuration de l'inventaire S3 et de l'exportation des analyses S3.

JSON

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryAndAnalyticsExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "111122223333",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Création de la configuration des rapports d'inventaire S3

Catalogage et analyse de vos données avec l'inventaire S3 crée des listes des objets figurant dans un compartiment S3 et des métadonnées de chaque objet. L'autorisation `s3:PutInventoryConfiguration` permet à un utilisateur de créer une configuration d'inventaire comprenant tous les champs de métadonnées d'objet disponibles par défaut et de spécifier le compartiment de destination où stocker cet inventaire. Un utilisateur disposant d'un accès en lecture

aux objets du compartiment de destination peut accéder à tous les champs de métadonnées d'objet disponibles dans ce rapport d'inventaire. Pour plus d'informations sur les champs de métadonnées disponibles dans S3 Inventory, consultez Liste d'inventaire Amazon S3.

Pour empêcher un utilisateur de configurer un rapport d'inventaire S3, supprimez l'autorisation `s3:PutInventoryConfiguration` de l'utilisateur.

Certains champs de métadonnées d'objet dans les configurations des rapports d'inventaire S3 sont facultatifs. En d'autres termes, ils sont disponibles par défaut, mais ils peuvent être restreints lorsque vous accordez l'autorisation `s3:PutInventoryConfiguration` à un utilisateur. Vous pouvez contrôler si les utilisateurs peuvent inclure ces champs de métadonnées facultatifs dans leurs rapports à l'aide de la clé de condition `s3:InventoryAccessibleOptionalFields`. Pour obtenir la liste des champs de métadonnées facultatifs disponibles dans l'inventaire S3, consultez OptionalFields dans la Référence d'API Amazon Simple Storage Service.

Pour autoriser un utilisateur à créer une configuration d'inventaire avec des champs de métadonnées facultatifs spécifiques, utilisez la clé de condition `s3:InventoryAccessibleOptionalFields` afin d'affiner les conditions de votre politique de compartiment.

L'exemple de politique suivant accorde à un utilisateur (*Ana*) l'autorisation de créer une configuration d'inventaire de manière conditionnelle. Dans cette politique, la condition `ForAllValues:StringEquals` utilise la clé de condition `s3:InventoryAccessibleOptionalFields` pour spécifier les deux champs de métadonnées facultatifs autorisés, à savoir `Size` et `StorageClass`. Ainsi, lorsqu'*Ana* créera une configuration d'inventaire, les seuls champs de métadonnées facultatifs qu'elle pourra inclure seront `Size` et `StorageClass`.

JSON

```
{
 "Id": "InventoryConfigPolicy",
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowInventoryCreationConditionally",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action":
    "s3:PutInventoryConfiguration",
```

```
    "Resource":
     "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
    "Condition": {
     "ForAllValues:StringEquals": {
      "s3:InventoryAccessibleOptionalFields": [
         "Size",
         "StorageClass"
         ]
       }
     }
    }
  ]
}
```

Pour empêcher un utilisateur de configurer un rapport d'inventaire S3 comprenant des champs de métadonnées facultatifs spécifiques, ajoutez une instruction `Deny` explicite à la politique du compartiment source. L'exemple de politique de compartiment suivant interdit à l'utilisatrice *Ana* de créer une configuration d'inventaire dans le compartiment source *DOC-EXAMPLE-SOURCE-BUCKET* avec les champs de métadonnées `ObjectAccessControlList` ou `ObjectOwner` facultatifs. L'utilisatrice *Ana* pourra toujours créer une configuration d'inventaire avec d'autres champs de métadonnées facultatifs.

```
{
 "Id": "InventoryConfigSomeFields",
 "Version": "2012-10-17",
 "Statement": [{
   "Sid": "AllowInventoryCreation",
   "Effect": "Allow",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
   },
   "Action": "s3:PutInventoryConfiguration",
   "Resource":
    "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",

  },
  {
   "Sid": "DenyCertainInventoryFieldCreation",
   "Effect": "Deny",
   "Principal": {
    "AWS": "arn:aws:iam::111122223333:user/Ana"
```

```
    },
    "Action": "s3:PutInventoryConfiguration",
    "Resource":
      "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET",
    "Condition": {
     "ForAnyValue:StringEquals": {
      "s3:InventoryAccessibleOptionalFields": [
         "ObjectOwner",
         "ObjectAccessControlList"
         ]
       }
     }
    }
 ]
}
```

> **Note**
>
> L'utilisation de la clé de condition `s3:InventoryAccessibleOptionalFields` dans les politiques de compartiment n'affecte pas la livraison des rapports d'inventaire basés sur les configurations d'inventaire existantes.

> **Important**
>
> Nous vous recommandons d'utiliser `ForAllValues` avec un effet `Allow` ou `ForAnyValue` avec un effet `Deny`, comme indiqué dans les exemples précédents.
> N'utilisez pas `ForAllValues` avec l'effet `Deny` ni `ForAnyValue` avec l'effet `Allow`, car ces combinaisons peuvent être trop restrictives et bloquer la suppression de la configuration de l'inventaire.
> Pour en savoir plus sur les opérateurs d'ensemble de conditions `ForAllValues` et `ForAnyValue`, consultez Clés de contexte à valeurs multiples dans le Guide de l'utilisateur IAM.

Exigence d'une MFA

Amazon S3 prend en charge l'accès aux API protégé par MFA, une fonction qui peut appliquer l'authentification multifactorielle (MFA) pour l'accès à vos ressources Amazon S3. L'authentification multifactorielle fournit un niveau de sécurité supplémentaire que vous pouvez appliquer à votre AWS

environnement. L'authentification MFA est une fonctionnalité de sécurité qui impose aux utilisateurs de prouver qu'ils détiennent physiquement un appareil d'authentification MFA en fournissant un code d'authentification MFA valide. Pour plus d'informations, consultez Authentification multifactorielle AWS. Vous pouvez exiger l'authentification MFA pour toutes les demandes d'accès à vos ressources Amazon S3.

Pour appliquer l'exigence d'authentification MFA, utilisez la clé de condition `aws:MultiFactorAuthAge` dans une politique de compartiment. Les utilisateurs IAM peuvent accéder aux ressources Amazon S3 à l'aide d'informations d'identification temporaires émises par le AWS Security Token Service (AWS STS). Vous fournissez le code MFA au moment de la demande AWS STS .

Quand Amazon S3 reçoit une demande d'authentification multifacteur, la clé de condition `aws:MultiFactorAuthAge` fournit une valeur numérique indiquant le temps écoulé (en secondes) depuis la création des informations d'identification temporaires. Si les informations d'identification temporaires fournies dans la demande n'ont pas été créées à l'aide d'un appareil d'authentification MFA, la valeur de cette clé est null (absente). Dans une politique de compartiment, vous pouvez ajouter une condition pour vérifier cette valeur, comme illustré dans l'exemple suivant.

Cet exemple de politique refuse toute opération Amazon S3 sur le dossier */taxdocuments* dans le compartiment *amzn-s3-demo-bucket* si la demande n'a pas été authentifiée à l'aide de l'authentification MFA. Pour en savoir plus sur MFA, consultez Utilisation de l'authentification multifacteur (MFA) dans AWS dans le Guide de l'utilisateur IAM.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true }}
      }
    ]
```

```
}
```

La condition `Null` figurant dans le bloc `Condition` équivaut à `true` si la valeur de la clé de condition `aws:MultiFactorAuthAge` est null, ce qui indique que les informations d'identification de sécurité temporaires figurant dans la demande ont été créées sans appareil d'authentification MFA.

La politique de compartiment suivante est une extension de la politique de compartiment précédente. La politique suivante comprend deux instructions de politique. Une déclaration accorde l'autorisation `s3:GetObject` sur un compartiment (*`amzn-s3-demo-bucket`*) à tous. Une autre déclaration limite encore plus l'accès au dossier *`amzn-s3-demo-bucket/taxdocuments`* du compartiment en requérant l'authentification MFA.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": { "Null": { "aws:MultiFactorAuthAge": true } }
      },
      {
        "Sid": "",
        "Effect": "Allow",
        "Principal": "*",
        "Action": ["s3:GetObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
      }
    ]
}
```

Vous pouvez éventuellement utiliser une condition numérique pour limiter la durée de validité de la clé `aws:MultiFactorAuthAge`. La durée que vous spécifiez pour la clé

`aws:MultiFactorAuthAge` est indépendante de la durée de vie de l'identifiant de sécurité temporaire utilisé pour authentifier la requête.

Par exemple, la politique de compartiment suivante, non seulement exige l'authentification MFA, mais vérifie également le temps écoulé depuis la création de la session temporaire. Cette stratégie refuse toute opération si la valeur de la clé `aws:MultiFactorAuthAge` indique que la session temporaire a été créée depuis plus d'une heure (3 600 secondes).

JSON

```
{
    "Version": "2012-10-17",
    "Id": "123",
    "Statement": [
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"Null": {"aws:MultiFactorAuthAge": true }}
      },
      {
        "Sid": "",
        "Effect": "Deny",
        "Principal": "*",
        "Action": "s3:*",
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/taxdocuments/*",
        "Condition": {"NumericGreaterThan": {"aws:MultiFactorAuthAge": 3600 }}
       },
       {
         "Sid": "",
         "Effect": "Allow",
         "Principal": "*",
         "Action": ["s3:GetObject"],
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
       }
    ]
 }
```

Empêcher les utilisateurs de supprimer des objets

Par défaut, les utilisateurs ne disposent d'aucune autorisation. Toutefois, lorsque vous créez des politiques, vous pouvez accorder à des utilisateurs des autorisations que vous n'aviez pas l'intention d'accorder. Pour éviter ces failles d'autorisation, vous pouvez écrire une stratégie d'accès plus stricte en ajoutant un refus explicite.

Pour empêcher explicitement des utilisateurs ou des comptes de supprimer des objets, vous devez ajouter les actions suivantes à une politique de compartiment : autorisations `s3:DeleteObject`, `s3:DeleteObjectVersion` et `s3:PutLifecycleConfiguration`. Ces trois actions sont nécessaires, car vous pouvez supprimer des objets soit en appelant explicitement les opérations d'API Gestion du cycle de vie des objets, soit en configurant leur cycle de vie (voir `DELETE Object`) afin qu'Amazon S3 puisse supprimer les objets lorsqu'ils arrivent à la fin de leur cycle de vie.

Dans l'exemple de politique suivant, vous refusez explicitement les autorisations `DELETE Object` à l'utilisatrice *`MaryMajor`*. L'instruction `Deny` explicite a toujours priorité sur n'importe quelle autre autorisation accordée.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "statement1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:GetObjectVersion",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
   "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    },
    {
      "Sid": "statement2",
      "Effect": "Deny",
```

```
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/MaryMajor"
      },
      "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutLifecycleConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket1",
     "arn:aws:s3:::amzn-s3-demo-bucket1/*"
      ]
    }
  ]
}
```

Exemples de politiques de compartiment utilisant des clés de condition

Vous pouvez utiliser le langage de la politique d'accès pour spécifier des conditions lorsque vous accordez des autorisations. Vous pouvez utiliser l'élément `Condition` facultatif ou le bloc `Condition` pour spécifier des conditions lorsqu'une politique est appliquée.

Pour les stratégies qui utilisent des clés de condition Amazon S3 pour les opérations d'objet et de compartiment, consultez les exemples suivants. Pour plus d'informations sur les clés de condition, consultez Clés de condition de politique pour Amazon S3. Pour obtenir la liste complète des actions, des clés de condition et des ressources Amazon S3 que vous pouvez spécifier dans les politiques, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Exemples : clés de condition Amazon S3 pour les opérations d'objet

Les exemples suivants montrent comment utiliser des clés de condition spécifiques à Amazon S3 pour les opérations au niveau des objets. Pour obtenir la liste complète des actions, des clés de condition et des ressources Amazon S3 que vous pouvez spécifier dans les politiques, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Plusieurs exemples de stratégies montrent comment vous pouvez utiliser des clés de condition avec des opérations PUT Object. Les opérations PUT Object autorisent les entêtes spécifiques à la liste de contrôle d'accès (ACL) que vous pouvez utiliser pour accorder des autorisations basées sur les listes ACL. En utilisant ces clés de condition, vous pouvez définir une condition pour exiger des autorisations d'accès spécifiques lorsque l'utilisateur charge un objet. Vous pouvez également accorder des autorisations basées sur l'ACL lors de l'opération. PutObjectAcl Pour plus d'informations, consultez PutObjectAcllle manuel Amazon S3 Amazon Simple Storage Service API Reference. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL).

Rubriques

- Exemple 1 : Octroyer l'autorisation s3:PutObject exigeant que les objets soient stockés en utilisant le chiffrement côté serveur
- Exemple 2 : Octroyer l'autorisation s3:PutObject pour copier des objets avec une restriction sur la source de copie
- Exemple 3 : Octroyer l'accès à une version spécifique d'un objet
- Exemple 4 : Octroi d'autorisations basées sur des balises d'objets
- Exemple 5 : Restriction de l'accès par l'ID de Compte AWS du propriétaire du compartiment
- Exemple 6 : Exiger une version minimale de TLS
- Exemple 7 : Exclure certains principaux d'une instruction Deny
- Exemple 8 : obliger les clients à télécharger des objets de manière conditionnelle en fonction des noms de clés des objets ou ETags

Exemple 1 : Octroyer l'autorisation **`s3:PutObject`** exigeant que les objets soient stockés en utilisant le chiffrement côté serveur

Supposons que le Compte A possède un compartiment. L'administrateur du compte souhaite accorder à Jane, une utilisatrice du compte A, l'autorisation de charger des objets avec cette condition : Jane doit toujours demander le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). L'administrateur du compte A peut utiliser la clé de condition `s3:x-amz-server-side-encryption` pour spécifier cette exigence, comme illustré. La paire clé-valeur du bloc `Condition` suivant spécifie la clé de condition `s3:x-amz-server-side-encryption` et SSE-S3 (`AES256`) comme type de chiffrement :

```
"Condition": {
     "StringNotEquals": {
         "s3:x-amz-server-side-encryption": "AES256"
     }}
```

Lorsque vous testez cette autorisation à l'aide du AWS CLI, vous devez ajouter le chiffrement requis à l'aide du `--server-side-encryption` paramètre, comme indiqué dans l'exemple suivant. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg --body c:
\HappyFace.jpg --server-side-encryption "AES256" --profile AccountAadmin
```

Exemple 2 : Octroyer l'autorisation **`s3:PutObject`** pour copier des objets avec une restriction sur la source de copie

Dans la demande PUT, quand vous spécifiez un objet source, il s'agit d'une opération de copie (voir CopyObject). En conséquence, le propriétaire du compartiment peut octroyer une autorisation utilisateur pour copier des objets avec des restrictions sur la source, par exemple :

- Autoriser la copie des objets uniquement à partir du compartiment source spécifié (par exemple, *amzn-s3-demo-source-bucket*)
- Autoriser la copie d'objets à partir du compartiment source spécifié et uniquement les objets dont le préfixe de nom de clé commence par *public/* (par exemple, *amzn-s3-demo-source-bucket/public/**)
- Autoriser la copie d'un objet spécifique uniquement à partir du compartiment source (par exemple, *amzn-s3-demo-source-bucket/example.jpg*)

La politique de compartiment suivante accorde à l'utilisateur (*Dave*) l'autorisation `s3:PutObject`. Cette politique lui permet de copier des objets uniquement à la condition que la demande inclue l'en-tête `s3:x-amz-copy-source` et que la valeur de l'en-tête spécifie le préfixe de nom de clé */amzn-s3-demo-source-bucket/public/**. Pour utiliser cet exemple de politique, remplacez *user input placeholders* par vos propres informations.

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
       {
            "Sid": "cross-account permission to user in your own account",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
        },
        {
            "Sid": "Deny your user permission to upload object if copy source is
 not /bucket/prefix",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-source-bucket/*",
            "Condition": {
                "StringNotLike": {
                    "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/*"
                }
            }
        }
    ]
}
```

Testez la politique à l'aide du AWS CLI

Vous pouvez tester l'autorisation à l'aide de la AWS CLI `copy-object` commande. Vous spécifiez la source en ajoutant le paramètre `--copy-source`, le préfixe du nom de clé doit correspondre au préfixe autorisé dans la stratégie. Vous devez fournir à l'utilisateur Dave les informations d'identification en utilisant le paramètre `--profile`. Pour plus d'informations sur la configuration du AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

```
aws s3api copy-object --bucket amzn-s3-demo-source-bucket --key HappyFace.jpg
--copy-source amzn-s3-demo-source-bucket/public/PublicHappyFace1.jpg --
profile AccountADave
```

Octroyer une autorisation pour copier uniquement un objet spécifique

La stratégie précédente utilise la condition `StringNotLike`. Pour accorder l'autorisation de copier uniquement un objet spécifique, vous devez remplacer la condition `StringNotLike` par `StringNotEquals`, puis spécifier la clé d'objet exacte, comme indiqué dans l'exemple suivant. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
"Condition": {
       "StringNotEquals": {
           "s3:x-amz-copy-source": "amzn-s3-demo-source-bucket/public/
PublicHappyFace1.jpg"
       }
}
```

Exemple 3 : Octroyer l'accès à une version spécifique d'un objet

Supposons que le compte A possède un compartiment pour lequel la gestion des versions est activée. Le compartiment a plusieurs versions de l'objet *`HappyFace.jpg`*. L'administrateur du compte A souhaite maintenant octroyer à l'utilisateur *`Dave`* l'autorisation d'obtenir uniquement une version spécifique de l'objet. Pour ce faire, l'administrateur du compte octroie à *`Dave`* l'autorisation `s3:GetObjectVersion` de manière conditionnelle, comme indiqué dans l'exemple suivant. La paire de clé-valeur dans le bloc `Condition` spécifie la clé de condition `s3:VersionId`. Dans ce cas, pour récupérer l'objet à partir du compartiment spécifié pour lequel la gestion des versions est activée, *`Dave`* doit connaître l'ID exact de la version de l'objet. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

Pour plus d'informations, consultez GetObject dans la Référence d'API Amazon Simple Storage Service.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
```

```
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg"
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::123456789012:user/Dave"
            },
            "Action": "s3:GetObjectVersion",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/HappyFace.jpg",
            "Condition": {
                "StringNotEquals": {
                    "s3:VersionId": "AaaHbAQitwiL_h47_44lRO2DDfLlBO5e"
                }
            }
        }
    ]
}
```

Testez la politique à l'aide du AWS CLI

Vous pouvez tester les autorisations définies dans cette politique en utilisant la AWS CLI `get-object` commande associée au `--version-id` paramètre pour identifier la version d'objet spécifique à récupérer. Cette commande récupère la version spécifiée de l'objet et l'enregistre dans le fichier *`OutputFile.jpg`*.

```
aws s3api get-object --bucket amzn-s3-demo-bucket --key HappyFace.jpg OutputFile.jpg --
version-id AaaHbAQitwiL_h47_44lRO2DDfLlBO5e --profile AccountADave
```

Exemple 4 : Octroi d'autorisations basées sur des balises d'objets

Pour obtenir des exemples sur l'utilisation des clés de condition de balisage d'objet avec des opérations Amazon S3, consultez Stratégies de balisage et de contrôle d'accès.

Exemple 5 : Restriction de l'accès par l'ID de Compte AWS du propriétaire du compartiment

Vous pouvez utiliser la clé de `s3:ResourceAccount` condition `aws:ResourceAccount` ou pour écrire des politiques de point de terminaison IAM ou de cloud privé virtuel (VPC) qui limitent l'accès des utilisateurs, des rôles ou des applications aux compartiments Amazon S3 détenus par un

identifiant spécifique. Compte AWS Vous pouvez utiliser cette clé de condition pour empêcher des clients de votre VPC d'accéder aux compartiments dont vous n'êtes pas propriétaire.

Sachez toutefois que certains AWS services dépendent de l'accès à des buckets AWS gérés. Par conséquent, l'utilisation de la clé `aws:ResourceAccount` ou `s3:ResourceAccount` dans votre politique IAM risque également d'avoir un impact sur l'accès à ces ressources. Pour plus d'informations, consultez les ressources suivantes :

- Restreindre l'accès aux compartiments dans un Compte AWS spécifié dans le Guide AWS PrivateLink
- Restreindre l'accès aux compartiments utilisés par Amazon ECR dans le Guide de l'utilisateur Amazon ECR
- Fournissez l'accès requis à Systems Manager pour les buckets Amazon S3 AWS gérés dans le Guide AWS Systems Manager

Pour plus d'informations sur les clés de condition `aws:ResourceAccount` et `s3:ResourceAccount`, et pour obtenir des exemples illustrant leur utilisation, consultez Limiter l'accès aux compartiments Amazon S3 détenus par des Comptes AWS spécifiques dans le blog AWS Storage.

Exemple 6 : Exiger une version minimale de TLS

Vous pouvez utiliser la clé de condition `s3:TlsVersion` afin d'écrire des politiques IAM, des politiques de point de terminaison de cloud privé virtuel (VPC) ou des politiques de compartiment pour restreindre l'accès des utilisateurs ou des applications aux compartiments Amazon S3 en fonction de la version TLS utilisée par le client. Vous pouvez utiliser cette clé de condition pour écrire des stratégies qui nécessitent une version TLS minimale.

> **Note**
>
> Lorsque AWS les services appellent d'autres AWS services en votre nom (service-to-service appels), certains contextes d'autorisation spécifiques au réseau sont supprimés, notamment `s3:TlsVersionaws:SecureTransport`, `aws:SourceIp` et. `aws:VpcSourceIp` Si votre politique utilise ces clés de condition avec des `Deny` instructions, les principaux AWS de service risquent d'être bloqués par inadvertance. Pour permettre aux AWS services de fonctionner correctement tout en respectant vos exigences de sécurité, excluez les principaux de service de vos `Deny` relevés en ajoutant la clé de `aws:PrincipalIsAWSService` condition avec une valeur `defalse`. Par exemple :

```
{
  "Effect": "Deny",
  "Action": "s3:*",
  "Resource": "*",
  "Condition": {
    "Bool": {
      "aws:SecureTransport": "false",
      "aws:PrincipalIsAWSService": "false"
    }
  }
}
```

Cette politique refuse l'accès aux opérations S3 lorsque le protocole HTTPS n'est pas utilisé (`aws:SecureTransport`c'est faux), mais uniquement pour les opérateurs non AWS liés au service. Cela garantit que vos restrictions conditionnelles s'appliquent à tous les principaux, à l'exception des principaux AWS de service.

Example

Cet exemple de politique de compartiment refuse les demandes `PutObject` des clients dont la version TLS est inférieure à 1.2, par exemple 1.1 ou 1.0. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericLessThan": {
```

```
                    "s3:TlsVersion": 1.2
                }
            }
        }
    ]
}
```

Example

Cet exemple de politique de compartiment autorise les demandes `PutObject` des clients dont la version TLS est supérieure à 1.1, par exemple 1.2, 1.3 ou plus :

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1",
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ],
            "Condition": {
                "NumericGreaterThan": {
                    "s3:TlsVersion": 1.1
                }
            }
        }
    ]
}
```

Exemple 7 : Exclure certains principaux d'une instruction **`Deny`**

La politique de compartiment suivante refuse l'accès `s3:GetObject` au compartiment *`amzn-s3-demo-bucket`*, à l'exception des principaux possédant le numéro de compte *`123456789012`*. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAccessFromPrincipalNotInSpecificAccount",
      "Principal": {
        "AWS": "*"
      },
      "Action": "s3:GetObject",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalAccount": [
            "123456789012"
          ]
        }
      }
    }
  ]
}
```

Exemple 8 : obliger les clients à télécharger des objets de manière conditionnelle en fonction des noms de clés des objets ou ETags

Avec les écritures conditionnelles, vous pouvez ajouter un en-tête supplémentaire à vos demandes `WRITE` afin de spécifier les conditions préalables à une opération S3. Cet en-tête spécifie une condition qui, si elle n'est pas remplie, entraînera l'échec de l'opération S3. Par exemple, vous pouvez empêcher le remplacement de données existantes en confirmant qu'aucun objet portant le

même nom de clé ne se trouve déjà dans votre compartiment lors du chargement de l'objet. Vous pouvez également vérifier la balise d'entité (ETag) d'un objet dans Amazon S3 avant d'écrire un objet.

Pour obtenir des exemples de politiques de compartiment qui utilisent les conditions d'une politique de compartiment pour appliquer les écritures conditionnelles, consultez the section called "Application d'écritures conditionnelles".

Exemples : clés de condition Amazon S3 pour les opérations sur les compartiments

Cette section fournit des exemples de politiques qui vous montrent comment utiliser des clés de condition spécifiques à Amazon S3 pour les opérations au niveau des compartiments.

Rubriques

- Exemple 1 : Accorder une autorisation s3:GetObject assortie d'une condition au niveau d'une adresse IP
- Exemple 2 : Obtention d'une liste d'objets dans un compartiment avec un préfixe spécifique
- Exemple 3 : Définition du nombre maximal de clés

Exemple 1 : Accorder une autorisation **`s3:GetObject`** assortie d'une condition au niveau d'une adresse IP

Vous pouvez autoriser les utilisateurs authentifiés à utiliser l'action `s3:GetObject` si la demande émane d'une plage d'adresses IP spécifique (par exemple, *`192.0.2.*`*), à l'exception de l'adresse IP que vous souhaitez exclure (par exemple, *`192.0.2.188`*). Dans le bloc `Condition`, les éléments `IpAddress` et `NotIpAddress` sont des conditions. Chacune est associée à une paire clé-valeur pour évaluation. Les deux paires clé-valeur de cet exemple utilisent la touche `aws:SourceIp` AWS large. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

> **Note**
>
> Les valeurs de clé `IPAddress` et `NotIpAddress` spécifiées dans le bloc `Condition` utilisent la notation CIDR comme décrit dans RFC 4632. Pour plus d'informations, consultez http://www.rfc-editor. org/rfc/rfc4632.txt.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "S3PolicyId1",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": "*",
            "Action":"s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition" : {
                "IpAddress" : {
                    "aws:SourceIp": "192.0.2.0/24"
                },
                "NotIpAddress" : {
                    "aws:SourceIp": "192.0.2.188/32"
                }
            }
        }
    ]
}
```

Vous pouvez également utiliser d'autres AWS clés de condition générales dans les politiques Amazon S3. Par exemple, vous pouvez spécifier les clés de condition `aws:SourceVpce` et `aws:SourceVpc` dans les stratégies de compartiment pour les points de terminaison de VPC. Pour plus d'exemples, consultez Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment.

> **Note**
>
> Pour certaines clés de condition AWS globales, seuls certains types de ressources sont pris en charge. Par conséquent, vérifiez si Amazon S3 prend en charge la clé de condition globale et le type de ressource que vous souhaitez utiliser, ou si vous devez utiliser une clé de condition spécifique à Amazon S3 à la place. Pour obtenir la liste complète des types de ressources et des clés de condition prises en charge pour Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Exemple 2 : Obtention d'une liste d'objets dans un compartiment avec un préfixe spécifique

Vous pouvez utiliser la clé de condition `s3:prefix` pour limiter la réponse de l'API ListObjectsV2 aux noms de clés avec un préfixe spécifique. Si vous êtes le propriétaire du compartiment, vous pouvez utiliser cette clé de condition pour restreindre un utilisateur afin qu'il ne puisse répertorier que le contenu d'un préfixe spécifique dans le compartiment. La clé de condition `s3:prefix` est utile si les objets du compartiment sont organisés par préfixe de nom de clé.

La console Amazon S3 utilise des préfixes de nom de clé pour afficher un concept de dossier. Seule la console prend en charge le concept de dossiers ; l'API Amazon S3 ne prend en charge que les compartiments et les objets. Par exemple, si vous avez deux objets avec les noms de clés *`public/object1.jpg`* et *`public/object2.jpg`*, la console affiche ces objets dans le dossier *`public`*. Dans l'API Amazon S3, il s'agit d'objets avec des préfixes, pas d'objets dans des dossiers. Pour plus d'informations sur l'utilisation de préfixes et de délimiteurs pour filtrer les autorisations d'accès, consultez Contrôle de l'accès à un compartiment avec des stratégies d'utilisateur.

Dans le scénario suivant, le propriétaire du compartiment et le compte parent auquel appartient l'utilisateur sont identiques. Ainsi, le propriétaire du compartiment peut utiliser une politique de compartiment ou une politique utilisateur. Pour plus d'informations sur les autres clés de condition que vous pouvez utiliser avec l'opération d'API `ListObjectsV2`, consultez ListObjectsV2.

> **Note**
>
> Si la gestion des versions est activée pour le compartiment et si vous souhaitez répertorier les objets dans ce compartiment, vous devez accorder l'autorisation `s3:ListBucketVersions` dans les politiques suivantes, au lieu de l'autorisation `s3:ListBucket`. L'autorisation `s3:ListBucketVersions` prend également en charge la clé de condition `s3:prefix`.

Stratégie utilisateur

La politique utilisateur suivante accorde l'autorisation `s3:ListBucket` (voir ListObjectsV2) avec une instruction `Condition` qui oblige l'utilisateur à spécifier un préfixe dans la demande avec la valeur

projects. Pour utiliser cet exemple de politique, remplacez *user input placeholders* par vos propres informations.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:ListBucket",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringEquals" : {
                 "s3:prefix": "projects"
             }
          }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringNotEquals" : {
                 "s3:prefix": "projects"
             }
          }
       }
    ]
}
```

L'instruction `Condition` restreint l'utilisateur pour qu'il ne puisse répertorier que les clés d'objet comportant le préfixe *projects*. L'instruction `Deny` explicite ajoutée refuse la demande de l'utilisateur de répertorier les clés avec un autre préfixe, quelles que soient les autres autorisations dont dispose cet utilisateur. Par exemple, il est possible que l'utilisateur obtienne l'autorisation de répertorier les clés d'objets sans aucune restriction, grâce aux mises à jour de la politique utilisateur précédente ou via une politique de compartiment. Comme les instructions `Deny` explicites ont

toujours la priorité sur les instructions `Allow`, si l'utilisateur essaie de répertorier des clés autres que celles qui ont le préfixe *`projects`*, la demande sera refusée.

Politique de compartiment

Si vous ajoutez l'élément `Principal` à la politique utilisateur ci-dessus, identifiant l'utilisateur, vous avez maintenant une politique de compartiment comme indiqué dans l'exemple suivant. Pour utiliser cet exemple de politique, remplacez *`user input placeholders`* par vos propres informations.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
         "Action":  "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringEquals" : {
                 "s3:prefix": "projects"
             }
          }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/bucket-owner"
         },
         "Action": "s3:ListBucket",
         "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
         "Condition" : {
             "StringNotEquals" : {
                 "s3:prefix": "projects"
             }
          }
       }
```

```
    ]
}
```

Testez la politique à l'aide du AWS CLI

Vous pouvez tester la politique à l'aide de la `list-object` AWS CLI commande suivante. Dans la commande, vous fournissez les informations d'identification utilisateur en utilisant le paramètre `--profile`. Pour plus d'informations sur la configuration et l'utilisation du AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

```
aws s3api list-objects --bucket amzn-s3-demo-bucket --prefix projects --
profile AccountA
```

Exemple 3 : Définition du nombre maximal de clés

Vous pouvez utiliser la clé de condition `s3:max-keys` pour définir le nombre maximum de clés qu'un demandeur peut renvoyer dans une demande ListObjectsV2 ou ListObjectVersions. Par défaut, les opérations d'API renvoient jusqu'à 1 000 clés. Pour obtenir la liste des opérateurs de conditions numériques que vous pouvez utiliser avec `s3:max-keys` et les exemples qui les accompagnent, consultez Opérateurs de conditions numériques dans le Guide de l'utilisateur IAM.

Politiques basées sur l'identité pour Amazon S3

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ni à modifier des ressources Amazon S3. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. 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. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

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 Amazon S3, y compris le format du ARNs pour chacun des types de ressources, consultez la section Actions, ressources et clés de condition pour Amazon S3 dans la référence d'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Rubriques

- Bonnes pratiques en matière de politiques
- Contrôle de l'accès à un compartiment avec des stratégies d'utilisateur
- Exemples de politiques basées sur l'identité pour Amazon S3

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si une personne peut créer, consulter ou supprimer des ressources Amazon S3 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 AWS 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.

Contrôle de l'accès à un compartiment avec des stratégies d'utilisateur

Cette démonstration explique comment les autorisations utilisateur fonctionnent avec Amazon S3. Dans cet exemple, vous créez un compartiment avec des dossiers. Vous créez ensuite des utilisateurs AWS Identity and Access Management IAM dans votre compartiment Amazon S3 Compte AWS et les dossiers qu'il contient et leur accordez des autorisations supplémentaires.

Rubriques

- Principes de base des compartiments et des dossiers
- Résumé de la procédure détaillée
- Préparation de la procédure détaillée
- Étape 1 : créer un compartiment
- Étape 2 : créer des utilisateurs IAM et un groupe
- Étape 3 : vérifier que les utilisateurs IAM ne disposent d'aucune autorisation
- Étape 4 : octroyer des autorisations au niveau du groupe
- Étape 5 : octroyer des autorisations spécifiques à l'utilisateur IAM Alice
- Étape 6 : octroyer des autorisations spécifiques à l'utilisateur IAM Bob
- Étape 7 : sécuriser le dossier Private

- Étape 8 : Nettoyage
- Ressources connexes

Principes de base des compartiments et des dossiers

Le modèle de données Amazon S3 est une structure horizontale : vous créez un compartiment et ce compartiment stocke des objets. Il n'existe aucune hiérarchie de sous-compartiments ou de sous-dossiers, mais vous pouvez émuler une hiérarchie de dossiers. Des outils tels que la console Amazon S3 peuvent présenter une vue de ces dossiers et sous-dossiers logiques dans votre compartiment.

La console montre qu'un compartiment nommé `companybucket` comporte trois dossiers, `Private`, `Development` et `Finance`, ainsi qu'un objet, `s3-dg.pdf`. La console utilise les noms d'objet (clés) pour créer une hiérarchie logique avec des dossiers et des sous-dossiers. Considérez les exemples suivants :

- Lorsque vous créez le dossier `Development`, la console crée un objet avec la clé `Development/`. Notez la barre oblique de fin (`/`) comme délimiteur.
- Lorsque vous chargez un objet nommé `Projects1.xls` dans le dossier `Development`, la console charge l'objet et lui fournit la clé `Development/Projects1.xls`.

  Dans la clé, `Development` est le préfixe et `/` le délimiteur. L'API Amazon S3 prend en charge les préfixes et les délimiteurs dans ses opérations. Par exemple, vous pouvez obtenir la liste de tous les objets d'un compartiment avec un préfixe et un délimiteur spécifiques. Dans la console, quand ouvrez le dossier `Development`, la console répertorie les objets de ce dossier. Dans l'exemple suivant, le dossier `Development` contient un seul objet.

  Lorsque la console répertorie le dossier `Development` dans le compartiment `companybucket`, elle envoie une demande à Amazon S3 dans laquelle elle spécifie le préfixe `Development` et le délimiteur `/`. La réponse de la console ressemble à une liste de dossiers du système de fichiers de votre ordinateur. L'exemple précédent montre que le compartiment `companybucket` possède un objet doté de la clé `Development/Projects1.xls`.

La console utilise des clés d'objet pour déduire une hiérarchie logique. Amazon S3 n'a pas de hiérarchie physique. Amazon S3 n'a que des compartiments contenant des objets dans une structure de fichier horizontale. Lorsque vous créez des objets à l'aide de l'API Amazon S3, vous pouvez utiliser des clés d'objet qui impliquent une hiérarchie logique. Lorsque vous créez une hiérarchie

logique d'objets, vous pouvez gérer l'accès aux dossiers individuels, comme le montre cette procédure détaillée.

Avant de commencer, veillez à vous familiariser avec le concept de contenu du compartiment de niveau racine. Supposez que votre compartiment `companybucket` contienne les objets suivants :

- `Private/privDoc1.txt`
- `Private/privDoc2.zip`
- `Development/project1.xls`
- `Development/project2.xls`
- `Finance/Tax2011/document1.pdf`
- `Finance/Tax2011/document2.pdf`
- `s3-dg.pdf`

Ces clés d'objet créent une hiérarchie logique avec `Private`, `Development` et `Finance` comme dossiers de niveau racine et `s3-dg.pdf` comme objet de niveau racine. Lorsque vous choisissez le nom du compartiment dans la console Amazon S3, les éléments de niveau racine apparaissent. La console montre les préfixes de niveau supérieur (`Private/`, `Development/` et `Finance/`) sous la forme de dossiers de niveau racine. La clé d'objet `s3-dg.pdf` n'a pas de préfixe et apparaît donc en tant qu'élément de niveau racine.

Résumé de la procédure détaillée

Dans cette procédure détaillée, vous créez un compartiment avec trois dossiers (`Private`, `Development` et `Finance`) dans celui-ci.

Vous avez deux utilisateurs, Alice et Bob. Vous souhaitez qu'Alice accède uniquement au dossier `Development` et que Bob accède uniquement au dossier `Finance`. Vous souhaitez garder le contenu du dossier `Private` privé. Dans cette procédure détaillée, vous gérez l'accès en créant des utilisateurs IAM (l'exemple utilise les noms d'utilisateur Alice et Bob) et vous leur octroyez les autorisations nécessaires.

IAM prend également en charge la création de groupes d'utilisateurs et l'octroi d'autorisations au niveau du groupe, qui s'appliquent à tous les utilisateurs du groupe. Cela vous aide à mieux gérer les autorisations. Pour cet exercice, Alice et Bob ont besoin de certaines autorisations communes. Vous allez donc créer un groupe nommé `Consultants` et ajouter Alice et Bob à ce groupe. Vous

commencerez par octroyer des autorisations en attachant une stratégie de groupe à ce groupe. Ensuite, vous ajouterez des autorisations spécifiques aux utilisateurs en attachant des stratégies aux utilisateurs spécifiques.

> **Note**
>
> Cette démonstration utilise `companybucket` comme nom de compartiment, Alice et Bob comme utilisateurs IAM, et `Consultants` comme nom de groupe. Comme Amazon S3 exige que les noms de compartiment soient uniques à l'échelle mondiale, vous devez remplacer le nom du compartiment par un nom de votre création.

Préparation de la procédure détaillée

Dans cet exemple, vous utilisez vos Compte AWS informations d'identification pour créer des utilisateurs IAM. Initialement, ces utilisateurs n'ont aucune autorisation. Vous octroyez de façon incrémentielle des autorisations à ces utilisateurs pour leur permettre d'effectuer des actions Amazon S3 spécifiques. Pour tester ces autorisations, vous vous connectez à la console avec les autorisations de chaque utilisateur. Au fur et à mesure que vous accordez des autorisations en tant que Compte AWS propriétaire et que vous testez des autorisations en tant qu'utilisateur IAM, vous devez vous connecter et vous déconnecter en utilisant à chaque fois des informations d'identification différentes. Vous pouvez effectuer ce test dans un seul navigateur, mais le processus sera accéléré si vous pouvez utiliser deux navigateurs différents. Utilisez un navigateur pour vous connecter à l' AWS Management Console aide de vos Compte AWS informations d'identification et un autre navigateur pour vous connecter aux informations d'identification utilisateur IAM.

Pour vous connecter à l' AWS Management Console aide de vos Compte AWS informations d'identification, rendez-vous sur https://console.aws.amazon.com/. Un utilisateur IAM ne peut pas se connecter en utilisant le même lien. Un utilisateur IAM doit utiliser une page de connexion prenant en charge IAM. En tant que propriétaire du compte, vous pouvez fournir ce lien à vos utilisateurs.

Pour plus d'informations sur IAM, consultez la page connexion à la AWS Management Console dans le Guide de l'utilisateur IAM.

Pour fournir un lien de connexion pour les utilisateurs IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau Navigation (Navigation), choisissez IAM Dashboard (Tableau de bord IAM).

3. Notez l'URL sous IAM users sign in link: (Lien de connexion des utilisateurs IAM). Vous donnerez ce lien aux utilisateurs IAM pour qu'ils se connectent à la console avec leur nom d'utilisateur et leur mot de passe IAM.

Étape 1 : créer un compartiment

Dans cette étape, vous allez vous connecter à la console Amazon S3 avec les informations d'identification de votre Compte AWS , créer un compartiment, y ajouter des dossiers et charger un ou deux exemples de document dans chaque dossier.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Créez un compartiment.

   Pour step-by-step obtenir des instructions, voirCréation d'un bucket à usage général.
3. Chargez un document dans le compartiment.

   Cet exercice suppose que vous disposez du document `s3-dg.pdf` au niveau racine de ce compartiment. Si vous chargez un autre document, inscrivez son nom de fichier à la place de `s3-dg.pdf`.
4. Ajoutez trois dossiers nommés `Private`, `Finance` et `Development` au compartiment.

   Pour step-by-step obtenir des instructions sur la création d'un dossier, consultez Organisation des objets dans la console Amazon S3 à l'aide de dossiers > dans le guide de l'utilisateur d'Amazon Simple Storage Service.
5. Chargez un ou deux documents dans chaque dossier.

   Pour cet exercice, supposons que vous avez chargé deux documents dans chaque dossier, de sorte que le compartiment possède des objets avec les clés suivantes :

   - `Private/privDoc1.txt`
   - `Private/privDoc2.zip`
   - `Development/project1.xls`
   - `Development/project2.xls`
   - `Finance/Tax2011/document1.pdf`
   - `Finance/Tax2011/document2.pdf`
   - `s3-dg.pdf`

Pour step-by-step obtenir des instructions, voirChargement d'objets.

Étape 2 : créer des utilisateurs IAM et un groupe

À présent, utilisez la console IAM pour ajouter deux utilisateurs IAM, Alice et Bob, à votre Compte AWS. Pour step-by-step obtenir des instructions, reportez-vous à la section Création d'un utilisateur IAM Compte AWS dans votre guide de l'utilisateur IAM.

Créez également un groupe administratif nommé `Consultants`. Ajoutez ensuite les deux utilisateurs au groupe. Pour step-by-step obtenir des instructions, consultez la section Création de groupes d'utilisateurs IAM.

> **Warning**
>
> Lorsque vous ajoutez des utilisateurs et un groupe, n'attachez aucune stratégie octroyant des autorisations à ces utilisateurs. Au début, les utilisateurs n'ont aucune autorisation. Dans les sections suivantes, vous allez octroyer des autorisations de façon incrémentielle. Vous devez tout d'abord vous assurer d'avoir attribué des mots de passe à ces utilisateurs IAM. Vous utiliserez les autorisations de ces utilisateurs pour tester les actions Amazon S3 et vérifier que ces autorisations fonctionnent comme prévu.

Pour step-by-step obtenir des instructions relatives à la création d'un nouvel utilisateur IAM, reportez-vous à la section Création d'un utilisateur IAM Compte AWS dans votre guide de l'utilisateur IAM. Lorsque vous créez les utilisateurs pour cette procédure, sélectionnez Accès àAWS Management Console et désactivez l'option Accès par programmation.

Pour step-by-step obtenir des instructions sur la création d'un groupe administratif, consultez la section Création de votre premier utilisateur et de votre premier groupe administrateur IAM dans le guide de l'utilisateur IAM.

Étape 3 : vérifier que les utilisateurs IAM ne disposent d'aucune autorisation

Si vous utilisez deux navigateurs, vous pouvez utiliser à présent le second navigateur pour vous connecter à la console en utilisant les autorisations d'un des utilisateurs IAM.

1. Utilisez le lien de connexion d'utilisateur IAM (consultez Pour fournir un lien de connexion pour les utilisateurs IAM) pour vous connecter à la AWS Management Console en utilisant les autorisations d'un des deux utilisateurs IAM.
2. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.

   Vérifiez que le message de la console s'affiche et vous indique que l'accès est refusé.

À présent, vous pouvez commencer octroyer des autorisations incrémentielles aux utilisateurs. En premier lieu, vous attacherez une stratégie de groupe octroyant les autorisations que les deux utilisateurs doivent posséder.

Étape 4 : octroyer des autorisations au niveau du groupe

Vous voulez que les utilisateurs soient en mesure d'effectuer les tâches suivantes :

- Répertorier tous les compartiments détenus par le compte parent. Pour cela, Bob et Alice doivent disposer de l'autorisation pour l'action `s3:ListAllMyBuckets`.
- Répertorier les éléments de niveau racine, les dossiers et les objets dans le compartiment `companybucket`. Pour cela, Bob et Alice doivent disposer de l'autorisation pour l'action `s3:ListBucket` sur le compartiment `companybucket`.

À présent, vous allez créer une stratégie qui octroie ces autorisations, puis vous l'attacherez au groupe `Consultants`.

Étape 4.1 : octroyer l'autorisation de répertorier tous les compartiments

Dans cette étape, vous allez créer une stratégie gérée qui octroie aux utilisateurs les autorisations minimales leur permettant de répertorier tous les compartiments détenus par le compte parent. Vous attacherez ensuite cette stratégie au groupe `Consultants`. Lorsque vous attachez la stratégie gérée à un utilisateur ou à un groupe, vous accordez à cet utilisateur ou à ce groupe l'autorisation d'obtenir la liste des compartiments détenus par le parent Compte AWS.

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.

> **Note**
>
> Comme vous octroyez des autorisations utilisateur, connectez-vous à l'aide des informations d'identification de votre Compte AWS , et non pas en tant qu'utilisateur IAM.

2. Créez la stratégie gérée.

   a. Dans le volet de navigation de gauche, sélectionnez Politiques, puis Créer une politique.

   b. Choisissez l'onglet JSON.

   c. Copiez la stratégie d'accès suivante et collez-la dans le champ de texte de stratégie.

      JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": ["s3:ListAllMyBuckets"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    }
  ]
}
```

      Une stratégie est un document JSON. Dans ce document, un élément `Statement` est un tableau d'objets, chacun décrivant une autorisation à l'aide d'une collection de paires de noms-valeurs. La stratégie précédente décrit une autorisation spécifique. L'élément `Action` spécifie le type d'accès. Dans la stratégie, l'élément `s3:ListAllMyBuckets` est une action Amazon S3 prédéfinie. Cette action couvre l'opération GET Service d'Amazon S3, qui renvoie la liste de tous les compartiments que l'expéditeur authentifié possède. La valeur de l'élément `Effect` détermine si une autorisation spécifique est accordée ou refusée.

   d. Choisissez Review Policy (Examiner une stratégie). Sur la page suivante, saisissez `AllowGroupToSeeBucketListInTheConsole`dans le champ Nom, puis choisissez Créer une stratégie.

> **Note**
>
> L'entrée Résumé affiche un message indiquant que la stratégie n'accorde pas d'autorisations. Vous pouvez ignorer ce message dans le cadre de cette procédure.

3. Attachez la stratégie gérée `AllowGroupToSeeBucketListInTheConsole` que vous avez créée au groupe `Consultants`.

   Pour step-by-step obtenir des instructions relatives à l'attachement d'une politique gérée, consultez la section Ajout et suppression d'autorisations d'identité IAM dans le guide de l'utilisateur IAM.

   Vous attachez des documents de stratégie aux utilisateurs IAM et aux groupes dans la console IAM. Comme vous voulez que les deux utilisateurs soient en mesure de répertorier les compartiments, vous attachez cette stratégie au groupe.

4. Testez l'autorisation.

   a. Utilisez le lien de connexion d'utilisateur IAM (consultez Pour fournir un lien de connexion pour les utilisateurs IAM) pour vous connecter à la console en utilisant les autorisations d'un des deux utilisateurs IAM.

   b. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.

      La console doit à présent répertorier tous les compartiments mais pas les objets figurant dans ces compartiments.

Étape 4.2 : permettre aux utilisateurs de répertorier le contenu de niveau racine d'un compartiment

Ensuite, autorisez tous les utilisateurs du groupe `Consultants` à répertorier les éléments de niveau racine du compartiment `companybucket`. Lorsqu'un utilisateur choisit le compartiment de l'entreprise dans la console Amazon S3, il peut voir les éléments de niveau racine figurant dans le compartiment.

> **Note**
>
> Cet exemple utilise `companybucket` à titre d'illustration. Vous devez utiliser le nom du compartiment que vous avez créé.

Pour comprendre la demande que la console envoie à Amazon S3 lorsque vous choisissez un nom de compartiment, la réponse qu'Amazon S3 renvoie et la manière dont la console interprète cette réponse, examinons les différentes étapes d'un peu plus près.

Lorsque vous choisissez un nom de compartiment, la console envoie la demande GET Bucket (List Objects) à Amazon S3. Cette demande inclut les paramètres suivants :

- le paramètre `prefix` avec une chaîne vide comme valeur ;
- le paramètre `delimiter` avec `/` comme valeur.

Voici un exemple de demande.

```
GET ?prefix=&delimiter=/ HTTP/1.1
Host: companybucket.s3.amazonaws.com
Date: Wed, 01 Aug  2012 12:00:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
```

Amazon S3 retourne une réponse qui inclut l'élément `<ListBucketResult/>`.

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>companybucket</Name>
  <Prefix></Prefix>
  <Delimiter>/</Delimiter>
   ...
  <Contents>
    <Key>s3-dg.pdf</Key>
    ...
  </Contents>
  <CommonPrefixes>
    <Prefix>Development/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Finance/</Prefix>
  </CommonPrefixes>
  <CommonPrefixes>
    <Prefix>Private/</Prefix>
  </CommonPrefixes>
</ListBucketResult>
```

L'objet de clé `s3-dg.pdf` ne contient pas la barre oblique (`/`) comme délimiteur et Amazon S3 retourne la clé dans l'élément `<Contents>`. Toutefois, toutes les autres clés dans notre exemple

de compartiment contiennent le délimiteur `/`. Amazon S3 regroupe ces clés et renvoie un élément `<CommonPrefixes>` pour chacune des valeurs de préfixe distinctes `Development/`, `Finance/` et `Private/` qui est une sous-chaîne du début de ces clés jusqu'à la première occurrence du délimiteur `/` spécifié.

La console interprète ce résultat et affiche les éléments de niveau racine sous la forme de trois dossiers et d'une clé d'objet.

Si Bob ou Alice ouvre le dossier Development (Développement), la console envoie la demande GET Bucket (List Objects) à Amazon S3 avec le préfixe `prefix` et les valeurs suivantes pour les paramètres `delimiter` :

- Le paramètre `prefix` avec la valeur `Development/`.
- Le paramètre `delimiter` avec la valeur « `/` ».

En réponse à cela, Amazon S3 renvoie les clés d'objet qui commencent par le préfixe spécifié.

```
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>companybucket</Name>
  <Prefix>Development</Prefix>
  <Delimiter>/</Delimiter>
   ...
  <Contents>
    <Key>Project1.xls</Key>
    ...
  </Contents>
  <Contents>
    <Key>Project2.xls</Key>
    ...
  </Contents>
</ListBucketResult>
```

La console affiche les clés d'objet.

A présent, revenez à l'octroi aux utilisateurs d'une autorisation pour répertorier les éléments de niveau racine du compartiment. Pour répertorier le contenu du compartiment, les utilisateurs ont besoin d'une autorisation pour appeler l'action `s3:ListBucket`, telle qu'illustrée dans la déclaration de stratégie ci-dessous. Pour s'assurer qu'ils ne voient que le contenu de niveau racine, vous ajoutez une condition stipulant que les utilisateurs doivent spécifier un paramètre `prefix` vide dans la demande (c'est-à-dire qu'ils ne sont pas autorisés à double-cliquer sur les dossiers de niveau

racine). Enfin, vous ajoutez une condition pour exiger un accès de type dossier en exigeant que les demandes des utilisateurs incluent le paramètre `delimiter` avec la valeur « `/` ».

```
{
  "Sid": "AllowRootLevelListingOfCompanyBucket",
  "Action": ["s3:ListBucket"],
  "Effect": "Allow",
  "Resource": ["arn:aws:s3:::companybucket"],
  "Condition":{
         "StringEquals":{
             "s3:prefix":[""], "s3:delimiter":["/"]
                       }
              }
}
```

Lorsque vous choisissez un compartiment sur la console Amazon S3, la console envoie d'abord la demande de localisation du compartiment GET pour savoir Région AWS où le compartiment est déployé. Ensuite, la console utilise le point de terminaison spécifique à la Région du compartiment pour envoyer la demande GET Bucket (List Objects). Par conséquent, si les utilisateurs doivent utiliser la console, vous devez octroyer l'autorisation pour l'action `s3:GetBucketLocation` telle qu'illustrée dans la déclaration de stratégie suivante.

```
{
   "Sid": "RequiredByS3Console",
   "Action": ["s3:GetBucketLocation"],
   "Effect": "Allow",
   "Resource": ["arn:aws:s3:::*"]
}
```

Pour permettre aux utilisateurs de répertorier le contenu de niveau racine d'un compartiment

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.

   Utilisez vos Compte AWS informations d'identification, et non celles d'un utilisateur IAM, pour vous connecter à la console.
2. Remplacez la stratégie gérée `AllowGroupToSeeBucketListInTheConsole` existante qui est attachée au groupe `Consultants` par la stratégie suivante, qui autorise également l'action `s3:ListBucket`. N'oubliez pas de remplacer *`companybucket`* dans l'élément `Resource` de la politique par le nom de votre compartiment.

Pour step-by-step obtenir des instructions, consultez la section Modification des politiques IAM dans le Guide de l'utilisateur IAM. Lorsque vous suivez les step-by-step instructions, veillez à suivre les étapes permettant d'appliquer vos modifications à toutes les entités principales auxquelles la politique est attachée.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
     {
       "Sid":
 "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
       "Action": [ "s3:ListAllMyBuckets", "s3:GetBucketLocation" ],
       "Effect": "Allow",
       "Resource": [ "arn:aws:s3:::*"  ]
     },
     {
       "Sid": "AllowRootLevelListingOfCompanyBucket",
       "Action": ["s3:ListBucket"],
       "Effect": "Allow",
       "Resource": ["arn:aws:s3:::companybucket"],
       "Condition":{
             "StringEquals":{
                    "s3:prefix":[""], "s3:delimiter":["/"]
                           }
                  }
     }
  ]
}
```

3. Testez les autorisations mises à jour.

   a. Utilisez le lien de connexion d'utilisateur IAM (voir Pour fournir un lien de connexion pour les utilisateurs IAM) pour vous connecter à la AWS Management Console.

      Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.

   b. Choisissez le compartiment que vous avez créé ; la console affiche les éléments de niveau racine du compartiment. Si vous choisissez un dossier dans le compartiment, vous

ne pourrez pas voir le contenu du dossier, car vous n'avez pas encore été octroyé ces autorisations.

Ce test réussit lorsque les utilisateurs utilisent la console Amazon S3. Lorsque vous choisissez sur un compartiment dans la console, l'implémentation de la console envoie une demande qui inclut le paramètre `prefix` avec une chaîne vide comme valeur et le paramètre `delimiter` avec la valeur « `/` ».

Étape 4.3 : récapitulatif de la stratégie de groupe

L'effet net de la stratégie de groupe que vous avez ajoutée est d'octroyer aux utilisateurs IAM Alice et Bob les autorisations minimales suivantes :

- Répertorier tous les compartiments détenus par le compte parent.
- Voir les éléments de niveau racine dans le compartiment `companybucket`.

Toutefois, les utilisateurs ont une marge de manœuvre encore limitée. Vous octroyez ensuite des autorisations spécifiques à l'utilisateur, comme suit :

- Autorisez Alice à obtenir et placer des objets dans le dossier `Development`.
- Autorisez Bob à obtenir et placer des objets dans le dossier `Finance`.

Dans le cadre des autorisations spécifiques à l'utilisateur, vous attachez une stratégie à un utilisateur spécifique et non pas au groupe. Dans la section suivante, vous octroyez à Alice l'autorisation de travailler dans le dossier `Development`. Vous pouvez répéter cette procédure pour octroyer une autorisation similaire à Bob pour lui permettre de travailler dans le dossier `Finance`.

Étape 5 : octroyer des autorisations spécifiques à l'utilisateur IAM Alice

À présent, vous octroyez des autorisations supplémentaires à Alice pour qu'elle puisse voir le contenu du dossier `Development`, ainsi qu'obtenir et placer des objets dans ce dossier.

Étape 5.1 : octroyer une autorisation à l'utilisateur IAM Alice pour répertorier le contenu du dossier Development

Pour qu'Alice répertorie le contenu du dossier `Development`, vous devez appliquer une politique à l'utilisatrice Alice. Cette politique doit octroyer une autorisation pour l'action `s3:ListBucket` sur le compartiment `companybucket`, à condition que la demande inclue le préfixe `Development/`.

Vous voulez que cette stratégie soit appliquée uniquement à l'utilisateur Alice. Vous devez donc une stratégie en ligne. Pour de plus amples informations sur les politiques en ligne, consultez Politiques gérées et politiques en ligne dans le Guide de l'utilisateur IAM.

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.

   Utilisez vos Compte AWS informations d'identification, et non celles d'un utilisateur IAM, pour vous connecter à la console.

2. Créez une stratégie en ligne pour octroyer à l'utilisateur Alice l'autorisation de répertorier le contenu du dossier `Development`.

   a. Dans le volet de navigation de gauche, choisissez Utilisateurs.

   b. Choisissez sur le nom d'utilisateur Alice.

   c. Sur la page des détails de l'utilisateur, choisissez l'onglet Autorisations, puis Ajouter une stratégie en ligne.

   d. Choisissez l'onglet JSON.

   e. Copiez la politique suivante et collez-la dans le champ de texte de politique.

      JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "AllowListBucketIfSpecificPrefixIsIncludedInRequest",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{  "StringLike":{"s3:prefix":["Development/*"] }
       }
    }
  ]
}
```

   f. Choisissez Review Policy (Examiner une stratégie). Sur la page suivante, saisissez un nom dans le champ Nom, puis choisissez Créer une stratégie.

3. Testez la modification des autorisations d'Alice :

a. Utilisez le lien de connexion d'utilisateur IAM (voir Pour fournir un lien de connexion pour les utilisateurs IAM) pour vous connecter à la AWS Management Console.

b. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.

c. Dans la console Amazon S3, vérifiez qu'Alice peut voir la liste des objets dans le dossier `Development/` du compartiment.

   Lorsque l'utilisateur choisit le dossier `/Development` pour afficher la liste des objets qu'il contient, la console Amazon S3 envoie la demande `ListObjects` à Amazon S3 avec le préfixe `/Development`. Comme l'utilisateur obtient l'autorisation de voir la liste des objets avec le préfixe `Development` et le délimiteur `/`, Amazon S3 renvoie la liste des objets avec le préfixe de clé `Development/`, et la console affiche cette liste.

Étape 5.2 : octroyer des autorisations à l'utilisateur IAM Alice pour obtenir et placer des objets dans le dossier Development

Pour qu'Alice puisse obtenir et placer des objets dans le dossier `Development`, elle a besoin d'une autorisation pour appeler les actions `s3:GetObject` et `s3:PutObject`. Les déclarations de stratégie suivantes octroient ces autorisations, à condition que la demande inclue le paramètre `prefix` avec la valeur `Development/`.

```
{
    "Sid":"AllowUserToReadWriteObjectData",
    "Action":["s3:GetObject", "s3:PutObject"],
    "Effect":"Allow",
    "Resource":["arn:aws:s3:::companybucket/Development/*"]
 }
```

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

   Utilisez vos Compte AWS informations d'identification, et non celles d'un utilisateur IAM, pour vous connecter à la console.

2. Modifiez la stratégie en ligne que vous avez créée à l'étape précédente.

   a. Dans le panneau de navigation de gauche, choisissez Utilisateurs.

   b. Choisissez sur le nom d'utilisateur Alice.

c. Dans la page des détails, sélectionnez l'onglet Autorisations et développez la section Stratégies en ligne.

d. En regard du nom de la stratégie que vous avez créée à l'étape précédente, choisissez Modifier la stratégie.

e. Copiez la stratégie suivante et collez-la dans le champ de texte de la stratégie pour remplacer la stratégie existante.

JSON

```
{
     "Version": "2012-10-17",
     "Statement":[
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      }
   ]
}
```

3. Testez la stratégie mise à jour :

a. Utilisez le lien de connexion d'utilisateur IAM (voir Pour fournir un lien de connexion pour les utilisateurs IAM) pour vous connecter à la AWS Management Console.

b. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.

c. Dans la console Amazon S3, vérifiez qu'Alice peut à présent ajouter un objet et télécharger un objet dans le dossier `Development`.

Étape 5.3 : refuser explicitement à l'utilisateur IAM Alice les autorisations pour tout autre dossier du compartiment

L'utilisateur Alice peut à présent répertorier le contenu de niveau racine dans le compartiment `companybucket`. Elle peut également obtenir et placer des objets dans le dossier `Development`. Si vous souhaitez réellement renforcer les autorisations d'accès, vous pouvez refuser explicitement à Alice l'accès aux autres dossiers du compartiment. S'il existe une autre stratégie (politique de compartiment ou liste ACL) qui accorde à Alice l'accès à d'autres dossiers du compartiment, ce refus explicite a priorité sur ces autorisations.

Vous pouvez ajouter la déclaration suivante à la stratégie de l'utilisateur Alice. Elle exige que toutes les demandes envoyées par Alice à Amazon S3 incluent le paramètre `prefix`, dont la valeur peut être `Development/*` ou une chaîne vide.

```
{
   "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
   "Action": ["s3:ListBucket"],
   "Effect": "Deny",
   "Resource": ["arn:aws:s3:::companybucket"],
   "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                  "Null"         : {"s3:prefix":false }
    }
}
```

Deux expressions conditionnelles figurent dans le bloc `Condition`. Les résultats de ces expressions conditionnelles sont associés à l'aide du `AND` logique. Si les deux conditions son vraies, le résultat de la combinaison combinée est vrai (true). Comme `Effect` dans cette stratégie est défini sur `Deny`, lorsque la `Condition` a la valeur true, les utilisateurs ne peuvent pas effectuer l'`Action` spécifiée.

- L'expression conditionnelle `Null` garantit que les demandes d'Alice incluent le paramètre `prefix`.

  Le paramètre `prefix` requiert un accès de type dossier. Si vous envoyez une demande sans le paramètre `prefix`, Amazon S3 renvoie toutes les clés d'objet.

  Si la demande inclut le paramètre `prefix` avec une valeur null, l'expression prend la valeur true, et le bloc entier `Condition` est défini sur true. Vous devez autoriser une chaîne vide comme valeur du paramètre `prefix`. Nous avons vu dans la discussion précédente qu'autoriser la chaîne null permet à Alice de récupérer les éléments de niveau racine du compartiment, comme le fait la

console dans la discussion précédente. Pour plus d'informations, consultez Étape 4.2 : permettre aux utilisateurs de répertorier le contenu de niveau racine d'un compartiment.

- L'expression conditionnelle `StringNotLike` garantit que si la valeur du paramètre `prefix` est spécifiée et n'est pas `Development/*`, la demande échoue.

Suivez les étapes de la section précédente et mettez à jour à nouveau la stratégie en ligne que vous avez créée pour l'utilisateur Alice.

Copiez la stratégie suivante et collez-la dans le champ de texte de la stratégie pour remplacer la stratégie existante.

JSON

```
{
   "Version": "2012-10-17",
   "Statement":[
      {
         "Sid":"AllowListBucketIfSpecificPrefixIsIncludedInRequest",
         "Action":["s3:ListBucket"],
         "Effect":"Allow",
         "Resource":["arn:aws:s3:::companybucket"],
         "Condition":{
            "StringLike":{"s3:prefix":["Development/*"]
            }
         }
      },
      {
        "Sid":"AllowUserToReadWriteObjectDataInDevelopmentFolder",
        "Action":["s3:GetObject", "s3:PutObject"],
        "Effect":"Allow",
        "Resource":["arn:aws:s3:::companybucket/Development/*"]
      },
      {
         "Sid": "ExplicitlyDenyAnyRequestsForAllOtherFoldersExceptDevelopment",
         "Action": ["s3:ListBucket"],
         "Effect": "Deny",
         "Resource": ["arn:aws:s3:::companybucket"],
         "Condition":{  "StringNotLike": {"s3:prefix":["Development/*",""] },
                        "Null"         : {"s3:prefix":false }
          }
      }
```

```
    ]
}
```

Étape 6 : octroyer des autorisations spécifiques à l'utilisateur IAM Bob

À présent, vous voulez accorder à Bob une autorisation sur le dossier `Finance`. Suivez la procédure que vous avez utilisée précédemment pour accorder des autorisations à Alice, mais remplacez le dossier `Development` par le dossier `Finance`. Pour step-by-step obtenir des instructions, voirÉtape 5 : octroyer des autorisations spécifiques à l'utilisateur IAM Alice.

Étape 7 : sécuriser le dossier Private

Dans cet exemple, vous n'avez que deux utilisateurs. Vous avez accordé toutes les autorisations minimales requises au niveau du groupe et accordé des autorisations au niveau de l'utilisateur seulement lorsque ces autorisations étaient réellement requises au niveau d'un utilisateur individuel. Cette approche aide à réduire au maximum l'effort de gestion des autorisations. Lorsque le nombre d'utilisateurs augmente, la gestion des autorisations peut devenir fastidieuse. Par exemple, vous ne voulez pas que les utilisateurs de cet exemple accèdent au contenu du dossier `Private`. Comment s'assurer de ne pas accorder accidentellement une autorisation utilisateur d'accès au dossier `Private` ? Vous devez ajouter une stratégie qui refuse explicitement l'accès à ce dossier. Un refus explicite a priorité sur toutes les autres autorisations.

Pour vous assurer que le dossier `Private` reste privé, vous pouvez ajouter les deux déclarations de refus suivantes à la stratégie de groupe :

- Ajoutez la déclaration suivante pour refuser explicitement toute action sur les ressources dans le dossier `Private` (`companybucket/Private/*`).

  ```
  {
    "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
    "Action": ["s3:*"],
    "Effect": "Deny",
    "Resource":["arn:aws:s3:::companybucket/Private/*"]
  }
  ```

- Vous refusez également l'autorisation pour l'action visant à répertorier les objets lorsque la demande spécifie le préfixe `Private/`. Dans la console, si Bob ou Alice ouvre le dossier `Private`, avec cette stratégie, Amazon S3 renvoie une réponse d'erreur.

  ```
  {
  ```

```
  "Sid": "DenyListBucketOnPrivateFolder",
  "Action": ["s3:ListBucket"],
  "Effect": "Deny",
  "Resource": ["arn:aws:s3:::*"],
  "Condition":{
      "StringLike":{"s3:prefix":["Private/"]}
   }
}
```

Remplacez la stratégie de groupe `Consultants` par une stratégie mise à jour qui inclut les déclarations de refus précédentes. Après l'application de la stratégie mise à jour, aucun des utilisateurs du groupe ne peut accéder au dossier `Private` de votre compartiment.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

   Utilisez vos Compte AWS informations d'identification, et non celles d'un utilisateur IAM, pour vous connecter à la console.

2. Remplacez la stratégie gérée `AllowGroupToSeeBucketListInTheConsole` existante qui est attachée au groupe `Consultants` par la stratégie suivante. N'oubliez pas de remplacer *`companybucket`* dans la stratégie par le nom de votre compartiment.

   Pour obtenir des instructions, consultez Modification des politiques gérées par le client dans le Guide de l'utilisateur IAM. Lorsque vous suivez ces instructions, veillez à suivre les consignes pour appliquer vos modifications à toutes les entités principales auxquelles la stratégie est attachée.

   JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid":
 "AllowGroupToSeeBucketListAndAlsoAllowGetBucketLocationRequiredForListBucket",
      "Action": ["s3:ListAllMyBuckets", "s3:GetBucketLocation"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::*"]
    },
```

```
    {
      "Sid": "AllowRootLevelListingOfCompanyBucket",
      "Action": ["s3:ListBucket"],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::companybucket"],
      "Condition":{
          "StringEquals":{"s3:prefix":[""]}
       }
    },
    {
      "Sid": "RequireFolderStyleList",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringNotEquals":{"s3:delimiter":"/"}
       }
     },
    {
      "Sid": "ExplictDenyAccessToPrivateFolderToEveryoneInTheGroup",
      "Action": ["s3:*"],
      "Effect": "Deny",
      "Resource":["arn:aws:s3:::companybucket/Private/*"]
    },
    {
      "Sid": "DenyListBucketOnPrivateFolder",
      "Action": ["s3:ListBucket"],
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::*"],
      "Condition":{
          "StringLike":{"s3:prefix":["Private/"]}
       }
    }
  ]
}
```

Étape 8 : Nettoyage

Pour effectuer le nettoyage, ouvrez la console IAM, puis supprimez les utilisateurs Alice et Bob. Pour step-by-step obtenir des instructions, consultez la section Suppression d'un utilisateur IAM dans le guide de l'utilisateur IAM.

Pour vous assurer que le stockage ne vous est plus facturé, vous devez également supprimer les objets et le compartiment que vous avez créés pour cet exercice.

Ressources connexes

- Gestion des politiques IAM dans le Guide de l'utilisateur IAM

Exemples de politiques basées sur l'identité pour Amazon S3

Cette section présente plusieurs exemples de politiques basées sur l'identité AWS Identity and Access Management (IAM) pour contrôler l'accès à Amazon S3. Pour obtenir des exemples de politiques de compartiment (politiques basées sur les ressources), consultez Politiques de compartiment pour Amazon S3. Pour plus d'informations sur le langage des politiques IAM, consultez Politiques, stratégies et autorisations dans Amazon S3.

Les exemples de politique suivants fonctionnent si vous les testez par programmation. Cependant, pour les utiliser avec la console Amazon S3, vous devez accorder des autorisations supplémentaires qui sont requises par la console. Pour des informations sur l'utilisation de stratégies comme celles-ci avec la console Amazon S3, consultez Contrôle de l'accès à un compartiment avec des stratégies d'utilisateur.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Rubriques

- Autoriser un accès utilisateur IAM à l'un de vos compartiments
- Autoriser chaque utilisateur IAM à accéder à un dossier dans un compartiment
- Autoriser un groupe à avoir un dossier partagé dans Amazon S3
- Autoriser tous vos utilisateurs à lire des objets dans une partie d'un compartiment
- Autoriser un partenaire à déposer des fichiers dans une partie spécifique d'un compartiment
- Restriction de l'accès aux compartiments Amazon S3 dans un Compte AWS spécifique
- Restriction de l'accès aux compartiments Amazon S3 au sein de votre unité organisationnelle
- Restriction de l'accès aux compartiments Amazon S3 au sein de votre organisation
- Octroi d'une autorisation permettant de récupérer la configuration PublicAccessBlock d'un Compte AWS

- Restriction de la création de compartiments à une seule région

Autoriser un accès utilisateur IAM à l'un de vos compartiments

Dans cet exemple, vous souhaitez accorder à un utilisateur IAM l' Compte AWS accès à l'un de vos compartiments et lui permettre d'ajouter*amzn-s3-demo-bucket1*, de mettre à jour et de supprimer des objets.

En plus de l'octroi des autorisations `s3:PutObject`, `s3:GetObject` et `s3:DeleteObject` à l'utilisateur, la stratégie octroie aussi les autorisations `s3:ListAllMyBuckets`, `s3:GetBucketLocation` et `s3:ListBucket`. Ces conditions supplémentaires sont requises par la console. De la même manière, les actions `s3:PutObjectAcl` et `s3:GetObjectAcl` sont nécessaires pour que les objets puissent être copiés, coupés et collés dans la console. Pour afficher un exemple qui octroie les autorisations aux utilisateurs et qui les teste en utilisant la console, consultez Contrôle de l'accès à un compartiment avec des stratégies d'utilisateur.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action": "s3:ListAllMyBuckets",
         "Resource":"*"
      },
      {
         "Effect":"Allow",
         "Action":["s3:ListBucket","s3:GetBucketLocation"],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1"
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetObject",
            "s3:GetObjectAcl",
            "s3:DeleteObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*"
```

```
      }
   ]
}
```

Autoriser chaque utilisateur IAM à accéder à un dossier dans un compartiment

Dans cet exemple, vous voulez que deux utilisateurs IAM, Mary et Carlos, aient accès à votre compartiment, *amzn-s3-demo-bucket1*, de sorte qu'ils puissent ajouter, mettre à jour et supprimer des objets. Cependant, vous souhaitez restreindre l'accès de chaque utilisateur à un seul préfixe (dossier) dans le compartiment. Vous pouvez créer des dossiers avec des noms qui correspondent à leur nom d'utilisateur.

```
amzn-s3-demo-bucket1
   Mary/
   Carlos/
```

Pour uniquement octroyer à chaque utilisateur l'accès à son dossier, vous pouvez écrire une stratégie pour chaque utilisateur et l'attacher individuellement. Par exemple, vous pouvez attacher la politique suivante à l'utilisateur Mary pour lui octroyer des autorisations spécifiques à Amazon S3 sur le dossier *amzn-s3-demo-bucket1*/*Mary*.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/Mary/*"
      }
   ]
}
```

Vous pouvez alors attacher une stratégie similaire à l'utilisateur Carlos, en spécifiant le dossier *Carlos* dans la valeur `Resource`.

Au lieu d'attacher des politiques à des utilisateurs individuels, vous pouvez en écrire une seule qui utilise une variable de politique, puis attacher la politique à un groupe. Vous devez d'abord créer un groupe et ajouter Mary et Carlos à ce groupe. L'exemple de stratégie suivant octroie un ensemble d'autorisations Amazon S3 dans le dossier *amzn-s3-demo-bucket1*`/${aws:username}`. Lorsque la politique sera évaluée, la variable de politique `${aws:username}` sera remplacée par le nom utilisateur du demandeur. Par exemple, si Mary envoie une demande pour placer un objet, l'opération est autorisée uniquement si Mary télécharge l'objet dans le dossier *amzn-s3-demo-bucket1*`/Mary`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
   ]
}
```

> **Note**
>
> Lorsque vous utilisez des variables de politique, vous devez spécifier explicitement la version `2012-10-17` de la politique. La version par défaut du langage de politique IAM, 2008-10-17, ne prend pas en charge les variables de stratégie.

Si vous souhaitez tester la politique précédente sur la console Amazon S3, la console nécessite des autorisations supplémentaires, comme indiqué dans la politique suivante. Pour en savoir plus sur la façon dont la console utilise ces autorisations, consultez Contrôle de l'accès à un compartiment avec des stratégies d'utilisateur.

JSON

```
{
 "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowGroupToSeeBucketListInTheConsole",
      "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    },
    {
      "Sid": "AllowRootLevelListingOfTheBucket",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{
            "StringEquals":{
                    "s3:prefix":[""], "s3:delimiter":["/"]
                           }
                }
    },
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Action": "s3:ListBucket",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Condition":{  "StringLike":{"s3:prefix":["${aws:username}/*"] }
       }
    },
      {
     "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
        "Effect":"Allow",
        "Action":[
```

```
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/${aws:username}/*"
      }
   ]
}
```

> **Note**
>
> Dans la version 2012-10-17 de la stratégie, les variables de stratégie commencent par $. Ce changement de syntaxe peut potentiellement créer un conflit si votre clé d'objet (nom d'objet) inclut un $.
> Pour éviter ce conflit, spécifiez le caractère $ en utilisant `${$}`. Par exemple, pour inclure la clé d'objet `my$file` dans une politique, spécifiez `my${$}file`.

Bien que les noms d'utilisateur IAM soient des identifiants conviviaux et compréhensibles, il n'est pas nécessaire qu'ils soient uniques à l'échelle mondiale. Par exemple, si l'utilisateur Carlos quitte l'organisation et qu'un autre Carlos la rejoint, le nouvel employé Carlos pourrait accéder aux informations de l'ancien employé Carlos.

Au lieu d'utiliser des noms d'utilisateur, vous pouvez créer des dossiers basés sur l'utilisateur IAM. IDs Chaque ID d'utilisateur IAM est unique. Dans ce cas, vous devez modifier la stratégie précédente pour utiliser la variable de stratégie `${aws:userid}`. Pour plus d'informations sur les identifiants utilisateur, consultez Identificateurs IAM dans le Guide de l'utilisateur IAM.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
```

```
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/home/${aws:userid}/*"
      }
   ]
}
```

Autoriser des utilisateurs non IAM (utilisateurs d'application mobile) à accéder à des dossiers dans un compartiment

Supposons que vous souhaitez développer une application mobile, un jeu qui stocke les données utilisateur dans un compartiment S3. Pour chaque utilisateur d'application, vous souhaitez créer un dossier dans votre compartiment. Vous souhaitez aussi limiter l'accès de chaque utilisateur à son propre dossier. Mais vous ne pouvez pas créer de dossier avant qu'une personne télécharge votre application et commence à jouer au jeu, car vous n'avez pas son ID utilisateur.

Dans ce cas, vous pouvez demander que les utilisateurs se connectent à votre application en utilisant des fournisseurs d'identité publics tels que Login with Amazon, Facebook ou Google. Une fois que les utilisateurs se sont connectés à votre application via l'un de ces fournisseurs, ils ont un ID utilisateur que vous pouvez utiliser afin de créer des dossiers spécifiques aux utilisateurs au moment de l'exécution.

Vous pouvez ensuite utiliser la fédération d'identité Web AWS Security Token Service pour intégrer les informations du fournisseur d'identité à votre application et obtenir des informations de sécurité temporaires pour chaque utilisateur. Vous pouvez ensuite créer des politiques IAM qui permettent à l'application d'accéder à votre compartiment et d'effectuer des opérations comme la création de dossiers spécifiques à l'utilisateur et le chargement de données. Pour plus d'informations sur la fédération d'identités Web, consultez À propos de la fédération d'identité Web dans le Guide de l'utilisateur IAM.

Autoriser un groupe à avoir un dossier partagé dans Amazon S3

Le fait d'attacher la stratégie suivante au groupe octroie à tous les membres du groupe l'accès au dossier suivant dans Amazon S3 : *amzn-s3-demo-bucket1*/share/marketing. Les membres du groupe sont uniquement autorisés à accéder aux autorisations spécifiques à Amazon S3 indiquées dans la stratégie et uniquement pour les objets dans le dossier spécifié.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/share/marketing/*"
      }
   ]
}
```

Autoriser tous vos utilisateurs à lire des objets dans une partie d'un compartiment

Dans cet exemple, vous créez un groupe appelé *`AllUsers`*, qui contient tous les utilisateurs IAM que possède le Compte AWS. Vous attachez ensuite une stratégie qui donne au groupe l'accès à `GetObject` et à `GetObjectVersion`, mais uniquement pour les objets dans le dossier *`amzn-s3-demo-bucket1`*`/readonly`.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/readonly/*"
      }
   ]
```

```
}
```

Autoriser un partenaire à déposer des fichiers dans une partie spécifique d'un compartiment

Dans cet exemple, vous créez un groupe appelé *AnyCompany* qui représente une société partenaire. Vous créez un utilisateur IAM pour la personne ou l'application spécifique de la société partenaire ayant besoin d'un accès, puis vous placez l'utilisateur dans le groupe.

Vous attachez ensuite une politique qui donne au groupe l'accès `PutObject` au dossier suivant dans le compartiment :

amzn-s3-demo-bucket1/uploads/anycompany

Vous voulez empêcher le groupe *AnyCompany* de faire quoi que soit d'autre avec le compartiment et vous ajoutez donc une instruction qui refuse explicitement l'autorisation à toutes les actions Amazon S3 à l'exception de `PutObject` sur n'importe quelle ressource Amazon S3 du Compte AWS.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":"s3:PutObject",
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      },
      {
         "Effect":"Deny",
         "Action":"s3:*",
         "NotResource":"arn:aws:s3:::amzn-s3-demo-bucket1/uploads/anycompany/*"
      }
   ]
}
```

Restriction de l'accès aux compartiments Amazon S3 dans un Compte AWS spécifique

Si vous voulez vous assurer que vos principaux Amazon S3 accèdent uniquement aux ressources qui se trouvent dans un environnement sécurisé Compte AWS, vous pouvez restreindre l'accès. Par exemple, cette politique IAM basée sur une identité utilise un effet `Deny` pour bloquer l'accès

aux actions Amazon S3, sauf si la ressource Amazon S3 concernée appartient au compte *222222222222*. Pour empêcher le principal IAM Compte AWS d'accéder aux objets Amazon S3 en dehors du compte, joignez la politique IAM suivante :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyS3AccessOutsideMyBoundary",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": [
            "222222222222"
          ]
        }
      }
    }
  ]
}
```

> **Note**
>
> Cette politique ne remplace pas vos contrôles d'accès IAM existants, car elle n'accorde aucun accès. Cette politique agit plutôt comme une barrière de protection supplémentaire pour vos autres autorisations IAM, quelles que soient les autorisations accordées par d'autres politiques IAM.

Assurez-vous de remplacer l'ID de compte *222222222222* dans la politique par votre propre Compte AWS. Pour appliquer une politique à plusieurs comptes tout en conservant cette restriction, remplacez l'ID de compte par la clé de condition `aws:PrincipalAccount`. Cette condition exige que le principal et la ressource soient dans le même compte.

Restriction de l'accès aux compartiments Amazon S3 au sein de votre unité organisationnelle

Si vous avez configuré une unité organisationnelle (UO) AWS Organizations, vous souhaiterez peut-être restreindre l'accès au compartiment Amazon S3 à une partie spécifique de votre organisation. Dans cet exemple, nous utiliserons la clé `aws:ResourceOrgPaths` pour restreindre l'accès au compartiment Amazon S3 à une unité organisationnelle de votre organisation. Dans cet exemple, l'ID de l'unité organisationnelle est *`ou-acroot-exampleou`*. Assurez-vous de remplacer cette valeur dans votre propre politique par votre propre unité d'organisation IDs.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "AllowS3AccessOutsideMyBoundary",
       "Effect": "Allow",
       "Action": [
         "s3:*"
       ],
       "Resource": "*",
       "Condition": {
         "ForAllValues:StringNotLike": {
           "aws:ResourceOrgPaths": [
             "o-acorg/r-acroot/ou-acroot-exampleou/"
           ]
         }
       }
     }
   ]
 }
```

> **Note**
>
> Cette politique n'accorde aucun accès. Au lieu de cela, cette politique sert de backstop pour vos autres autorisations IAM, empêchant vos principaux d'accéder aux objets Amazon S3 en dehors d'une limite définie par l'unité organisationnelle.

La politique refuse l'accès aux actions Amazon S3, sauf si l'objet Amazon S3 auquel on accède se trouve dans l'unité organisationnelle *ou-acroot-exampleou* de votre organisation. La condition de politique IAM a besoin de `aws:ResourceOrgPaths`, clé de condition à valeurs multiples, pour contenir un des chemins d'unité organisationnelle répertoriés. La politique utilise l'`ForAllValues:StringNotLike`opérateur pour comparer les valeurs de `aws:ResourceOrgPaths` à celles répertoriées OUs sans distinction majuscules/majuscules.

Restriction de l'accès aux compartiments Amazon S3 au sein de votre organisation

Pour restreindre l'accès aux objets Amazon S3 au sein de votre organisation, attachez une politique IAM à la racine de l'organisation, en l'appliquant à tous les comptes de votre organisation. Pour demander à vos principaux IAM de respecter cette règle, utilisez une politique de contrôle des services (SCP). Si vous choisissez d'utiliser une SCP, veillez à bien tester la SCP avant d'attacher la politique à la racine de l'organisation.

Dans l'exemple de politique suivant, l'accès est refusé aux actions Amazon S3, sauf si l'objet Amazon S3 accédé se trouve dans la même organisation que le principal IAM qui y accède :

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
     {
       "Sid": "DenyS3AccessOutsideMyBoundary",
       "Effect": "Deny",
       "Action": [
         "s3:*"
       ],
       "Resource": "arn:aws:s3:::*/*",
       "Condition": {
         "StringNotEquals": {
           "aws:ResourceOrgID": "${aws:PrincipalOrgID}"
         }
       }
     }
   ]
 }
```

> **Note**
>
> Cette politique n'accorde aucun accès. Cette politique agit plutôt comme un backstop pour vos autres autorisations IAM, empêchant vos principaux d'accéder à tous les objets Amazon S3 en dehors de votre organisation. Cette politique s'applique également aux ressources Amazon S3 créées après l'entrée en vigueur de la politique.

Dans cet exemple, la condition de politique IAM nécessite que `aws:ResourceOrgID` et `aws:PrincipalOrgID` soient égaux les uns aux autres. Avec cette exigence, le principal qui fait la demande et la ressource accédée doivent faire partie de la même organisation.

Octroi d'une autorisation permettant de récupérer la configuration PublicAccessBlock d'un Compte AWS

L'exemple de politique utilisateur suivant octroie l'autorisation `s3:GetAccountPublicAccessBlock` à un utilisateur. Pour ces autorisations, définissez la valeur `Resource` sur `"*"`. Pour plus d'informations sur ARNs les ressources, consultezRessources de politique pour Amazon S3.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action":[
            "s3:GetAccountPublicAccessBlock"
         ],
         "Resource":[
            "*"
         ]
       }
    ]
}
```

Restriction de la création de compartiments à une seule région

Supposons qu'un Compte AWS administrateur souhaite autoriser son utilisateur (Dave) à créer un bucket uniquement dans la région Amérique du Sud (São Paulo). L'administrateur de compte peut attacher la stratégie d'utilisateur suivant octroyant l'autorisation `s3:CreateBucket` avec une condition comme indiqué. La paire de clé-valeur dans le bloc `Condition` spécifie la clé `s3:LocationConstraint` et la Région `sa-east-1` comme sa valeur.

> **Note**
>
> Dans cet exemple, le propriétaire du compartiment octroie l'autorisation à un de ses utilisateurs. Par conséquent une politique de compartiment ou une stratégie d'utilisateur peuvent être utilisées. Cette exemple illustre une stratégie d'utilisateur.

Pour obtenir la liste des régions Amazon S3, consultez Régions et points de terminaison dans Références générales AWS.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:CreateBucket",
         "Resource": "arn:aws:s3:::*",
         "Condition": {
             "StringLike": {
                 "s3:LocationConstraint": "sa-east-1"
             }
         }
       }
    ]
}
```

Ajouter un refus explicite

La stratégie précédente limite la création, par l'utilisateur, d'un compartiment dans une autre Région à l'exception de `sa-east-1`. Toutefois, une autre stratégie peut accorder à cet utilisateur l'autorisation de créer des compartiments dans une autre Région. Par exemple, si l'utilisateur appartient à un groupe, une stratégie peut être attachée à ce groupe, autorisant tous les utilisateurs du groupe à créer des compartiments dans une autre Région. Pour garantir que l'utilisateur n'obtienne pas l'autorisation de créer des compartiments dans une autre région, vous pouvez ajouter une instruction de refus explicite dans la politique ci-dessus.

L'instruction `Deny` utilise la condition `StringNotLike`. C'est-à-dire qu'une demande de création de compartiment est refusée si la contrainte d'emplacement n'est pas `sa-east-1`. Le refus explicite n'autorise pas l'utilisateur à créer un compartiment dans une autre région, quelles que soient les autres autorisations obtenues par l'utilisateur. La politique ci-dessous inclut une instruction de refus explicite.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"statement1",
         "Effect":"Allow",
         "Action": "s3:CreateBucket",
         "Resource": "arn:aws:s3:::*",
         "Condition": {
             "StringLike": {
                 "s3:LocationConstraint": "sa-east-1"
             }
         }
       },
      {
         "Sid":"statement2",
         "Effect":"Deny",
         "Action": "s3:CreateBucket",
         "Resource": "arn:aws:s3:::*",
         "Condition": {
             "StringNotLike": {
                 "s3:LocationConstraint": "sa-east-1"
             }
         }
       }
```

```
    ]
}
```

Testez la politique à l'aide du AWS CLI

Vous pouvez tester la politique à l'aide de la `create-bucket` AWS CLI commande suivante. Cet exemple utilise le fichier `bucketconfig.txt` pour spécifier la contrainte d'emplacement. Notez le chemin de fichiers Windows. Vous devez mettre à jour le nom du compartiment et le chemin comme approprié. Vous devez fournir les informations d'identification utilisateur en utilisant le paramètre `--profile`. Pour plus d'informations sur la configuration et l'utilisation du AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

```
aws s3api create-bucket --bucket examplebucket --profile AccountADave --create-bucket-
configuration file://c:/Users/someUser/bucketconfig.txt
```

Le fichier `bucketconfig.txt` spécifie la configuration comme suit.

```
{"LocationConstraint": "sa-east-1"}
```

Procédures détaillées qui utilisent des politiques pour gérer l'accès à vos ressources Amazon S3

Cette rubrique fournit les exemples de procédures suivants permettant l'accès aux ressources d'Amazon S3. Ces exemples utilisent le AWS Management Console pour créer des ressources (compartiments, objets, utilisateurs) et leur accorder des autorisations. Ces exemples montrent ensuite comment vérifier les autorisations à l'aide des outils de ligne de commande afin de vous éviter d'avoir à écrire un code. Nous fournissons des commandes en utilisant à la fois le AWS Command Line Interface (AWS CLI) et le AWS Tools for Windows PowerShell.

- Exemple 1 : propriétaire d'un compartiment accordant à ses utilisateurs des autorisations sur un compartiment

  Par défaut, les utilisateurs IAM que vous créez dans votre compte n'ont pas d'autorisation. Dans cet exercice, vous accordez une autorisation à un utilisateur pour exécuter des opérations de compartiments et d'objets.

- Exemple 2 : propriétaire d'un compartiment accordant à ses utilisateurs des autorisations entre comptes sur un compartiment

  Dans cet exercice, un propriétaire de compartiment, le compte A, accorde des autorisations d'accès intercompte à un autre Compte AWS, le compte B. Le compte B délègue ensuite ces autorisations aux utilisateurs dans son compte.

- Gestion des autorisations lorsque les propriétaires d'objets et de compartiments ne sont pas les mêmes

  Ces exemples de scénario décrivent un propriétaire de compartiment concédant des autorisations d'objets à d'autres, toutefois tous les objets du compartiment n'appartiennent pas à son propriétaire. De quelles autorisations le propriétaire du compartiment a besoin et comment peut-il déléguer ces autorisations ?

  Celui Compte AWS qui crée un bucket s'appelle le propriétaire du bucket. Le propriétaire peut accorder d'autres Comptes AWS autorisations pour télécharger des objets, et ceux Comptes AWS qui créent des objets en sont propriétaires. Le propriétaire du compartiment n'a aucune autorisation sur ces objets créés par d'autres Comptes AWS. Si le propriétaire du compartiment écrit une politique de compartiment permettant l'accès aux objets, cette politique ne s'applique pas aux objets détenus par d'autres comptes.

Dans ce cas, le propriétaire de l'objet doit d'abord accorder des autorisations au propriétaire du compartiment utilisant une liste ACL d'objet. Le propriétaire du bucket peut ensuite déléguer ces autorisations d'objets à d'autres personnes, à des utilisateurs de son propre compte ou à un autre Compte AWS, comme l'illustrent les exemples suivants.

- Exemple 3 : propriétaire d'un compartiment accordant des autorisations sur des objets qu'il ne possède pas

  Dans cet exercice, le propriétaire du compartiment obtient d'abord les autorisations du propriétaire de l'objet. Le propriétaire du compartiment délègue ensuite ces autorisations aux utilisateurs dans son propre compte.

- Exemple 4 : propriétaire d'un compartiment accordant des autorisations intercomptes à des objets qu'il ne possède pas

  Après avoir reçu les autorisations du propriétaire de l'objet, celui-ci ne peut pas déléguer d'autorisation à d'autres personnes Comptes AWS car la délégation entre comptes n'est pas prise en charge (voirDélégation d'autorisations). Au lieu de cela, le propriétaire du compartiment peut créer un rôle IAM autorisé à effectuer des opérations spécifiques (comme obtenir un objet) et autoriser un autre Compte AWS à assumer ce rôle. Toute personne occupant ce rôle peut ensuite accéder aux objets. Cet exemple montre comment un propriétaire du compartiment peut utiliser un rôle IAM pour permettre la délégation entre comptes.

Avant d'essayer les procédures d'exemples

Ces exemples utilisent le AWS Management Console pour créer des ressources et accorder des autorisations. Pour tester les autorisations, les exemples utilisent les outils de ligne de commande AWS CLI AWS Tools for Windows PowerShell, et vous n'avez donc pas besoin d'écrire de code. Afin de tester des autorisations, vous devez installer un de ces outils. Pour de plus amples informations, veuillez consulter Configuration des outils pour les procédures détaillées.

Par ailleurs, lorsque vous créez des ressources, ces exemples n'utilisent pas les informations d'identification d'utilisateur racine d'un Compte AWS. A la place, vous créez un administrateur pour ces comptes afin qu'il exécute ces tâches.

Utilisation d'un utilisateur administrateur pour créer des ressources et accorder des autorisations

AWS Identity and Access Management (IAM) déconseille l'utilisation des informations d'identification d'utilisateur root de votre Compte AWS pour effectuer des demandes. Il est préférable de créer un

rôle ou un utilisateur IAM, d'accorder un accès total à cet utilisateur et d'utiliser ses informations d'identification pour effectuer des demandes. Nous l'appelons rôle ou utilisateur administrateur. Pour plus d'informations, consultez Informations d'identification Utilisateur racine d'un compte AWS et identités IAM dans Références générales AWS et dans Bonnes pratiques IAM du Guide de l'utilisateur IAM.

Toutes les exemples de démonstration dans cette section utilisent les autorisations de l'utilisateur administrateur. Si vous n'avez pas créé d'utilisateur administrateur pour votre compte Compte AWS, les rubriques vous indiquent comment procéder.

Pour vous connecter à l' AWS Management Console aide des informations d'identification de l'utilisateur, vous devez utiliser l'URL de connexion de l'utilisateur IAM. La console IAM fournit cette URL pour votre Compte AWS. Les rubriques vous indiquent comment obtenir cette URL.

Configuration des outils pour les procédures détaillées

Les exemples d'introduction (voirProcédures détaillées qui utilisent des politiques pour gérer l'accès à vos ressources Amazon S3) utilisent le AWS Management Console pour créer des ressources et accorder des autorisations. Pour tester les autorisations, les exemples utilisent les outils de ligne de commande AWS Command Line Interface (AWS CLI) et AWS Tools for Windows PowerShell vous n'avez donc pas besoin d'écrire de code. Afin de tester des autorisations, vous devez installer un de ces outils.

Pour configurer le AWS CLI

1. Téléchargez et configurez l'interface AWS CLI. Pour obtenir des instructions, consultez les rubriques suivantes dans le Guide de l'utilisateur de l'interface AWS Command Line Interface :

   Installation ou mise à jour vers la dernière version de l' AWS Command Line Interface

   Premiers pas avec l' AWS Command Line Interface
2. Définir le profil par défaut.

   Vous stockez les informations d'identification de l'utilisateur dans le fichier de AWS CLI configuration. Créez un profil par défaut dans le fichier de configuration à l'aide de vos Compte AWS informations d'identification. Pour obtenir des instructions sur la recherche et la modification de votre fichier de AWS CLI configuration, consultez la section Paramètres du fichier de configuration et d'identification.

   ```
   [default]
   ```

```
aws_access_key_id = access key ID
aws_secret_access_key = secret access key
region = us-west-2
```

3. Vérifiez la configuration en saisissant la commande suivante à l'invite de commande. Ces deux commandes ne fournissent pas directement d'autorisations, par conséquent ce sont les informations du profil par défaut qui sont utilisées.

   - Essayez la commande `help`.

     ```
     aws help
     ```

   - Pour obtenir une liste de compartiments pour le compte configuré, utilisez la commande `aws s3 ls`.

     ```
     aws s3 ls
     ```

Pendant que vous effectuez les procédures détaillées, vous créerez des utilisateurs et enregistrerez des informations d'identification utilisateur dans les fichiers de configuration, comme l'illustrent les exemples suivants. Ces profils portent les noms `AccountAadmin` et `AccountBadmin`.

```
[profile AccountAadmin]
aws_access_key_id = User AccountAadmin access key ID
aws_secret_access_key = User AccountAadmin secret access key
region = us-west-2

[profile AccountBadmin]
aws_access_key_id = Account B access key ID
aws_secret_access_key = Account B secret access key
region = us-east-1
```

Pour exécuter une commande avec ces informations d'identification utilisateur, ajoutez un paramètre `--profile` spécifiant le nom du profil. La AWS CLI commande suivante permet de récupérer une liste d'objets *`examplebucket`* et de spécifier le `AccountBadmin` profil.

```
aws s3 ls s3://examplebucket --profile AccountBadmin
```

Vous pouvez aussi configurer une série d'informations d'identification utilisateur en tant que profil par défaut en modifiant la variable d'environnement `AWS_DEFAULT_PROFILE` à l'invite de commande.

Ensuite, chaque fois que vous exécutez des AWS CLI commandes sans le `--profile` paramètre, le AWS CLI profil que vous avez défini dans la variable d'environnement est le profil par défaut.

```
$ export AWS_DEFAULT_PROFILE=AccountAadmin
```

Pour configurer AWS Tools for Windows PowerShell

1. Téléchargez et configurez l'interface AWS Tools for Windows PowerShell. Pour obtenir des instructions, consultez Installation d' AWS Tools for Windows PowerShell dans le Guide de l'utilisateur Outils AWS pour PowerShell .

   > **Note**
   >
   > Pour charger le AWS Tools for Windows PowerShell module, vous devez activer l'exécution PowerShell du script. Pour plus d'informations, consultez Activation de l'exécution du script dans le Guide de l'utilisateur Outils AWS pour PowerShell .

2. Pour ces procédures pas à pas, vous spécifiez les AWS informations d'identification par session à l'aide de la `Set-AWSCredentials` commande. La commande enregistre les informations d'identification dans un stockage permanent (paramètre `-StoreAs`).

   ```
   Set-AWSCredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -
   storeas string
   ```

3. Vérifier la configuration

   - Pour récupérer la liste des commandes disponibles pour effectuer des opérations Amazon S3, exécutez la commande `Get-Command`.

     ```
     Get-Command -module awspowershell -noun s3* -StoredCredentials string
     ```

   - Pour récupérer une liste d'objets dans un compartiment, exécutez la commande `Get-S3Object`.

     ```
     Get-S3Object -BucketName bucketname -StoredCredentials string
     ```

Pour obtenir la liste des commandes, consultez la section AWS Outils de référence pour les PowerShell applets de commande.

Vous êtes maintenant prêt à essayer les procédures détaillées. Suivez les liens fournis au début de chaque section.

Exemple 1 : propriétaire d'un compartiment accordant à ses utilisateurs des autorisations sur un compartiment

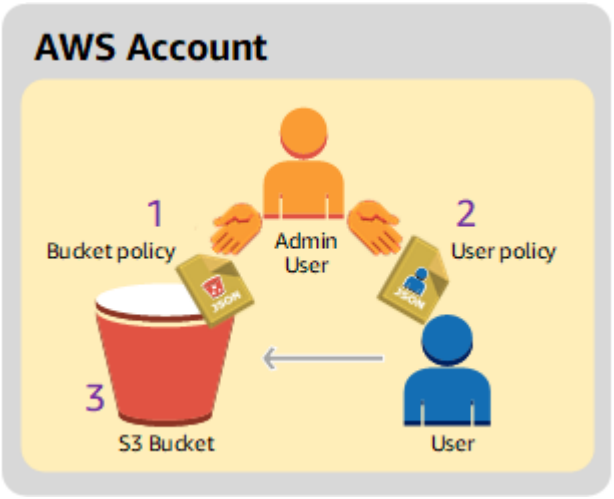
> **Important**
>
> Il est préférable d'accorder des autorisations à des rôles IAM plutôt qu'à des utilisateurs individuels. Pour plus d'informations sur l'octroi d'autorisations à des rôles IAM, consultez Fonctionnement des autorisations intercomptes et utilisation des rôles IAM.

Rubriques

- Préparation de la procédure détaillée
- Étape 1 : créer des ressources dans le compte A et accorder des autorisations
- Étape 2 : tester les autorisations

Dans cette procédure pas à pas, un utilisateur Compte AWS possède un bucket et le compte inclut un utilisateur IAM. Par défaut, l'utilisateur n'a aucune autorisation. Le compte parent doit accorder des autorisations à l'utilisateur pour que celui-ci puisse exécuter des tâches. Le propriétaire du compartiment et le compte parent sont identiques. Par conséquent, pour accorder à l'utilisateur des autorisations sur le compartiment, il Compte AWS peut utiliser une politique de compartiment, une politique utilisateur ou les deux. Le propriétaire du compte accorde certaines autorisations grâce à une politique de compartiment et d'autres autorisations grâce à une stratégie d'utilisateur.

Les étapes suivantes résument la procédure :



1. L'administrateur du compte crée une politique de compartiment qui accorde un ensemble d'autorisations à l'utilisateur.
2. L'administrateur du compte attache une stratégie d'utilisateur à l'utilisateur en accordant des autorisations supplémentaires.
3. L'utilisateur essaie ensuite les autorisations accordées via la politique de compartiment et utilisateur.

Pour cet exemple, vous aurez besoin d'un Compte AWS. Au lieu d'utiliser les informations d'identification d'utilisateur root du compte, vous créez un utilisateur administrateur (consultez Utilisation d'un utilisateur administrateur pour créer des ressources et accorder des autorisations). Nous faisons référence à l'utilisateur Compte AWS et à l'utilisateur administrateur comme indiqué dans le tableau suivant.

ID de compte	Compte désigné comme	Utilisateur administrateur du compte
1111-1111-1111	Compte A	AccountAadmin

> **Note**
>
> Dans cet exemple, l'utilisateur administrateur est AccountAadmin, ce qui fait référence au compte A, et non AccountAdmin.

Toutes les tâches de création d'utilisateurs et d'octroi d'autorisations sont effectuées dans la AWS Management Console. Pour vérifier les autorisations, la procédure pas à pas utilise les outils de ligne de commande AWS Command Line Interface (AWS CLI) et AWS Tools for Windows PowerShell vous n'avez donc pas besoin d'écrire de code.

Préparation de la procédure détaillée

1. Assurez-vous que vous disposez d'un Compte AWS et qu'il possède un utilisateur doté de privilèges d'administrateur.

   a. Inscrivez-vous pour un Compte AWS, si nécessaire. Nous appelons ce compte : Compte A.

      i. Accédez à https://aws.amazon.com/s3 et choisissez Créer un AWS compte.

ii. Suivez les instructions à l'écran.

AWS vous informera par e-mail lorsque votre compte sera actif et que vous pourrez l'utiliser.

b. Dans le compte A, créez un utilisateur administrateur, **`AccountAadmin`**. En utilisant les informations d'identification du Compte A, connectez-vous à la console IAM et procédez comme suit :

i. Créez l'utilisateur **`AccountAadmin`** et notez ses informations d'identification de sécurité.

Pour obtenir des instructions, consultez Création d'un utilisateur IAM dans votre Compte AWS dans le Guide de l'utilisateur IAM.

ii. Accordez des privilèges d'administrateur à AccountAadminen joignant une politique utilisateur donnant un accès complet.

Pour obtenir des instructions, consultez Gestion des politiques IAM dans le Guide de l'utilisateur IAM.

iii. Notez l'URL de connexion de l'utilisateur IAM pour. AccountAadmin Vous devez utiliser cette URL pour vous connecter sur la AWS Management Console. Pour plus d'informations sur l'emplacement de l'URL de connexion, voir Se connecter en AWS Management Console tant qu'utilisateur IAM dans le guide de l'utilisateur IAM. Notez l'URL pour chacun des comptes.

2. Configurez le AWS CLI ou le AWS Tools for Windows PowerShell. Assurez-vous d'enregistrer les autorisations de l'utilisateur administrateur comme suit :

- Si vous utilisez le AWS CLI, créez un profil dans le fichier de configuration. `AccountAadmin`
- Si vous utilisez le AWS Tools for Windows PowerShell, assurez-vous de stocker les informations d'identification de la session sous le nom`AccountAadmin`.

Pour obtenir des instructions, veuillez consulter Configuration des outils pour les procédures détaillées.

Étape 1 : créer des ressources dans le compte A et accorder des autorisations

À l'aide des informations d'identification de l'utilisateur figurant `AccountAadmin` dans le compte A et de l'URL de connexion spéciale de l'utilisateur IAM, connectez-vous au AWS Management Console et procédez comme suit :

1. Création des ressources d'un compartiment et d'un utilisateur IAM

   a. Dans la console Amazon S3, créez un compartiment. Notez l'endroit Région AWS dans lequel vous avez créé le bucket. Pour obtenir des instructions, veuillez consulter Création d'un bucket à usage général.

   b. Dans la console IAM, procédez comme suit :

      i. Créez un utilisateur nommé Dave.

         Pour step-by-step obtenir des instructions, consultez la section Création d'utilisateurs IAM (console) dans le guide de l'utilisateur IAM.

      ii. Notez les informations d'identification de `UserDave`.

      iii. Notez l'Amazon Resource Name (ARN) de l'utilisateur Dave. Dans la console IAM, sélectionnez l'utilisateur. L'onglet Récapitulatif fournit l'ARN utilisateur.

2. Octroyez les autorisations.

   Étant donné que le propriétaire du compartiment et le compte parent auquel appartient l'utilisateur sont identiques, ils Compte AWS peuvent accorder des autorisations à l'utilisateur en utilisant une politique de compartiment, une politique utilisateur ou les deux. Dans cet exemple, vous faites les deux. Si l'objet est également détenu par le même compte, le propriétaire du compartiment peut accorder des autorisations d'objet dans la politique de compartiment (ou une politique IAM).

   a. Dans la console Amazon S3, associez la politique de compartiment suivante à*`awsexamplebucket1`*.

      La stratégie possède deux énoncés.

      - Le premier énoncé accorde à Dave les autorisations d'opération sur le compartiment `s3:GetBucketLocation` et `s3:ListBucket`.
      - Le second énoncé accorde l'autorisation `s3:GetObject`. Etant donné que le Compte A détient l'objet, l'administrateur du compte peut accorder l'autorisation `s3:GetObject`.

Dans l'énoncé `Principal`, Dave est identifié par son ARN utilisateur. Pour en savoir plus sur les éléments de la stratégie, consultez Politiques, stratégies et autorisations dans Amazon S3.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Dave"
            },
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::awsexamplebucket1"
            ]
        },
        {
            "Sid": "statement2",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Dave"
            },
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::awsexamplebucket1/*"
            ]
        }
    ]
}
```

b. Créez une stratégie intégrée pour l'utilisateur Dave à l'aide de la stratégie suivante. La stratégie accorde à Dave l'autorisation `s3:PutObject`. Vous devez mettre à jour la stratégie en fournissant le nom du compartiment.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "PermissionForObjectOperations",
         "Effect": "Allow",
         "Action": [
            "s3:PutObject"
         ],
         "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*"
         ]
      }
   ]
}
```

Pour obtenir des instructions, reportez-vous IAMpolicies à la section Gestion du guide de l'utilisateur IAM. Notez que vous devez vous connecter sur la console grâce aux autorisations du Compte A.

Étape 2 : tester les autorisations

À l'aide des autorisations de Dave, vérifiez que les autorisations fonctionnent. Vous pouvez utiliser l'une des deux procédures suivantes.

Testez les autorisations à l'aide du AWS CLI

1. Mettez à jour le fichier de AWS CLI configuration en ajoutant le `UserDaveAccountA` profil suivant. Pour de plus amples informations, veuillez consulter Configuration des outils pour les procédures détaillées.

```
[profile UserDaveAccountA]
aws_access_key_id = access-key
```

```
aws_secret_access_key = secret-access-key
region = us-east-1
```

2. Vérifiez que Dave peut exécuter les opérations telles qu'elles sont accordées dans la stratégie d'utilisateur. Téléchargez un exemple d'objet à l'aide de la AWS CLI `put-object` commande suivante.

   Le paramètre `--body` de la commande identifie le fichier source à charger. Par exemple, si le fichier est à la racine du disque C: sur une machine Windows, vous spécifiez `c:\HappyFace.jpg`. Le paramètre `--key` fournit le nom de clé de l'objet.

   ```
   aws s3api put-object --bucket awsexamplebucket1 --key HappyFace.jpg --
   body HappyFace.jpg --profile UserDaveAccountA
   ```

   Exécutez la AWS CLI commande suivante pour obtenir l'objet.

   ```
   aws s3api get-object --bucket awsexamplebucket1 --key HappyFace.jpg OutputFile.jpg
    --profile UserDaveAccountA
   ```

Testez les autorisations à l'aide du AWS Tools for Windows PowerShell

1. Stockez les informations d'identification de Dave sous le nom `AccountADave`. Vous utilisez ensuite ces informations d'identification pour faire une demande `PUT` et `GET` sur un objet.

   ```
   set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
    AccountADave
   ```

2. Téléchargez un exemple d'objet à l'aide de la AWS Tools for Windows PowerShell `Write-S3Object` commande en utilisant les informations d'identification enregistrées par l'utilisateur Dave.

   ```
   Write-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file HappyFace.jpg
    -StoredCredentials AccountADave
   ```

   Téléchargez l'objet précédemment chargé.

   ```
   Read-S3Object -bucketname awsexamplebucket1 -key HappyFace.jpg -file Output.jpg -
   StoredCredentials AccountADave
   ```

Exemple 2 : propriétaire d'un compartiment accordant à ses utilisateurs des autorisations entre comptes sur un compartiment

> **Important**
>
> Il est préférable d'accorder des autorisations à des rôles IAM plutôt qu'à des utilisateurs individuels. Pour savoir comment procéder, consultez Fonctionnement des autorisations intercomptes et utilisation des rôles IAM.

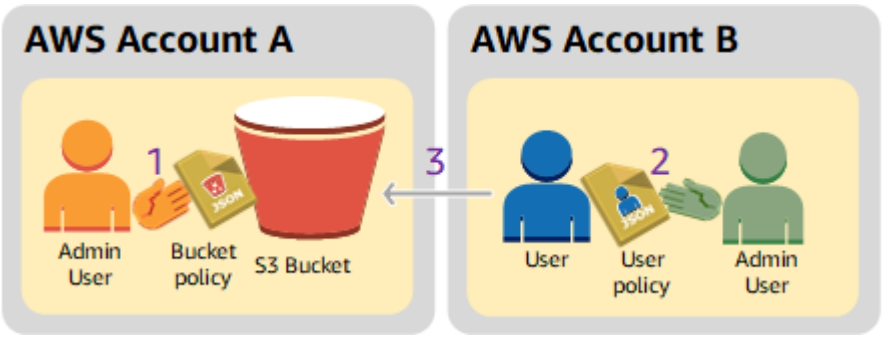
Rubriques

- Préparation de la procédure détaillée
- Étape 1 : réaliser les tâches du compte A
- Étape 2 : réaliser les tâches du compte B
- Étape 3 : (Facultatif) essayer le refus explicite
- Étape 4 : nettoyer

Un compte Compte AWS A, par exemple, peut accorder à un autre Compte AWS, le compte B, l'autorisation d'accéder à ses ressources, telles que des seaux et des objets. Le compte B peut ensuite déléguer ces autorisations aux utilisateurs du compte. Dans ce scénario fictif, le propriétaire d'un compartiment accorde une autorisation entre comptes à un autre compte pour lui permettre d'effectuer des opérations spécifiques sur un compartiment.

> **Note**
>
> Le compte A peut également accorder directement des autorisations à un utilisateur du compte B, par le biais d'une politique de compartiment. Toutefois, l'utilisateur aura toujours besoin de l'autorisation du compte parent (le compte B) auquel il appartient, même si ce compte n'a pas reçu d'autorisation du compte A. Tant que l'utilisateur dispose d'une autorisation accordée par le propriétaire de la ressource et par le compte parent, il pourra accéder à la ressource.

Les étapes suivantes résument la procédure à suivre :



1. L'utilisateur administrateur du compte A attache une politique de compartiment en accordant au compte B des autorisations intercomptes pour lui permettre d'effectuer des opérations spécifiques sur un compartiment.

   Notez que l'utilisateur administrateur du compte B hérite automatiquement des autorisations.
2. L'utilisateur administrateur du compte B attache une stratégie d'utilisateur à l'utilisateur en déléguant les autorisations qu'il a reçues du compte A.
3. L'utilisateur du compte B vérifie ensuite les autorisations en accédant à un objet dans le compartiment appartenant au compte A.

Pour cet exemple, vous avez besoin de deux comptes. Le tableau ci-dessous montre comment nous faisons référence à ces comptes et à leurs utilisateurs administrateurs. Conformément aux directives IAM (voir Utilisation d'un utilisateur administrateur pour créer des ressources et accorder des autorisations), nous n'utilisons pas les informations d'identification de l'utilisateur racine dans cette procédure détaillée. A la place, vous créez un utilisateur administrateur dans chaque compte et utilisez ces autorisations pour créer des ressources et leur accorder des autorisations.

Compte AWS ID	Compte désigné comme	Utilisateur administrateur du compte
1111-1111-1111	Compte A	AccountAadmin
2222-2222-2222	Compte B	AccountBadmin

Toutes les tâches de création d'utilisateurs et d'octroi d'autorisations sont effectuées dans la AWS Management Console. Pour vérifier les autorisations, la procédure pas à pas utilise les outils de ligne de commande AWS Command Line Interface (CLI) et AWS Tools for Windows PowerShell vous n'avez donc pas besoin d'écrire de code.

Préparation de la procédure détaillée

1. Assurez-vous que vous en avez deux Comptes AWS et que chaque compte possède un utilisateur administrateur, comme indiqué dans le tableau de la section précédente.

   a. Inscrivez-vous pour un Compte AWS, si nécessaire.

   b. Utilisez les informations d'identification du compte A pour vous connecter à la console IAM afin de créer l'utilisateur administrateur :

      i. Créez l'utilisateur **`AccountAadmin`** et notez les informations d'identification. Pour obtenir des instructions, consultez Création d'un utilisateur IAM dans votre Compte AWS dans le Guide de l'utilisateur IAM.

      ii. Accordez des privilèges d'administrateur à AccountAadminen joignant une politique utilisateur donnant un accès complet. Pour obtenir des instructions, consultez Utilisation de stratégies dans le Guide de l'utilisateur IAM.

   c. Lorsque vous êtes dans la console IAM, notez l'URL de connexion de l'utilisateur IAM sur le tableau de bord. Tous les utilisateurs du compte doivent utiliser cette URL pour se connecter à la AWS Management Console.

      Pour plus d'informations, consultez Comment les utilisateurs se connectent à votre compte dans le Guide de l'utilisateur IAM.

   d. Répétez l'étape précédente en utilisant les informations d'identification du compte B et créez l'utilisateur administrateur **`AccountBadmin`**.

2. Configurez le AWS Command Line Interface (AWS CLI) ou le AWS Tools for Windows PowerShell. Assurez-vous d'enregistrer les autorisations de l'utilisateur administrateur comme suit :

   - Si vous utilisez le AWS CLI, créez deux profils, `AccountAadmin` et`AccountBadmin`, dans le fichier de configuration.
   - Si vous utilisez le AWS Tools for Windows PowerShell, assurez-vous de stocker les informations d'identification de la session sous forme `AccountAadmin` et`AccountBadmin`.

   Pour obtenir des instructions, veuillez consulter Configuration des outils pour les procédures détaillées.

3. Enregistrez les autorisations de l'utilisateur administrateur, également appelées « profils ». Vous pouvez utiliser le nom de profil au lieu de spécifier des autorisations pour chaque commande

saisie. Pour de plus amples informations, veuillez consulter Configuration des outils pour les procédures détaillées.

a. Ajoutez des profils dans le fichier AWS CLI d'informations d'identification pour chacun des utilisateurs administrateurs `AccountAadmin` et `AccountBadmin` dans les deux comptes.

```
[AccountAadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1

[AccountBadmin]
aws_access_key_id = access-key-ID
aws_secret_access_key = secret-access-key
region = us-east-1
```

b. Si vous utilisez AWS Tools for Windows PowerShell, exécutez la commande suivante.

```
set-awscredentials –AccessKey AcctA-access-key-ID –SecretKey AcctA-secret-access-key –storeas AccountAadmin
set-awscredentials –AccessKey AcctB-access-key-ID –SecretKey AcctB-secret-access-key –storeas AccountBadmin
```

Étape 1 : réaliser les tâches du compte A

Étape 1.1 : Connectez-vous au AWS Management Console

À l'aide de l'URL de connexion utilisateur IAM pour le compte A, connectez-vous d'abord au compte en AWS Management Console tant qu'AccountAadminutilisateur. Cet utilisateur créera un compartiment et y attachera une stratégie.

Étape 1.2 : créer un compartiment

1. Dans la console Amazon S3, créez un compartiment. Cet exercice suppose que le bucket a été créé dans l'est des États-Unis (Virginie du Nord) Région AWS et qu'il porte un nom*amzn-s3-demo-bucket*.

   Pour obtenir des instructions, veuillez consulter Création d'un bucket à usage général.
2. Chargez un exemple d'objet dans le compartiment.

   Pour plus d'informations, consultez Étape 2 : charger un objet dans votre compartiment.

Étape 1.3 : attacher une politique de compartiment afin d'accorder des autorisations entre comptes au compte B

La politique du compartiment accorde les `s3:ListBucket` autorisations `s3:GetLifecycleConfiguration` et au compte B. On suppose que vous êtes toujours connecté à la console à l'aide des informations AccountAadmind'identification utilisateur.

1. Attachez la politique de compartiment suivante à *`amzn-s3-demo-bucket`*. Cette stratégie accorde au compte B une autorisation pour les actions `s3:GetLifecycleConfiguration` et `s3:ListBucket`.

   Pour obtenir des instructions, veuillez consulter Ajout d'une politique de compartiment à l'aide de la console Amazon S3.

   JSON

   ```
   {
      "Version": "2012-10-17",
      "Statement": [
         {
            "Sid": "Example permissions",
            "Effect": "Allow",
            "Principal": {
               "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
               "s3:GetLifecycleConfiguration",
               "s3:ListBucket"
            ],
            "Resource": [
               "arn:aws:s3:::amzn-s3-demo-bucket"
            ]
         }
      ]
   }
   ```

2. Vérifiez que le compte B (et donc son utilisateur administrateur) peut effectuer les opérations.

   - Vérifiez à l'aide du AWS CLI

     ```
     aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
     ```

```
aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --
profile AccountBadmin
```

- Vérifiez à l'aide du AWS Tools for Windows PowerShell

```
get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBadmin
get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
StoredCredentials AccountBadmin
```

Étape 2 : réaliser les tâches du compte B

L'administrateur du compte B va maintenant créer un utilisateur, Dave, et lui déléguer les autorisations reçues du compte A.

Étape 2.1 : Connectez-vous au AWS Management Console

À l'aide de l'URL de connexion utilisateur IAM pour le compte B, connectez-vous d'abord au compte en AWS Management Console tant qu'AccountBadminutilisateur.

Étape 2.2 : créer l'utilisateur Dave dans le compte B

Dans la console IAM, créez un utilisateur, **`Dave`**.

Pour obtenir des instructions, consultez Création d'utilisateurs IAM (console) dans le Guide de l'utilisateur IAM.

Étape 2.3 : déléguer les autorisations à l'utilisateur Dave

Créez une stratégie intégrée pour l'utilisateur Dave à l'aide de la stratégie suivante. Vous devrez mettre à jour la stratégie en fournissant le nom du compartiment.

Il est supposé que vous êtes connecté à la console à l'aide des informations AccountBadmind'identification utilisateur.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Example",
         "Effect": "Allow",
```

```
            "Action": [
               "s3:ListBucket"
            ],
            "Resource": [
               "arn:aws:s3:::example-s3-bucket;"
            ]
         }
      ]
}
```

Pour obtenir des instructions, consultez Gestion des politiques IAM dans le Guide de l'utilisateur IAM.

Étape 2.4 : tester les autorisations

Dans le compte B, Dave peut maintenant répertorier le contenu du compartiment *amzn-s3-demo-bucket* appartenant au compte A. Vous pouvez vérifier les autorisations via l'une des procédures suivantes.

Testez les autorisations à l'aide du AWS CLI

1. Ajoutez le `UserDave` profil au fichier de AWS CLI configuration. Pour plus d'informations sur le fichier de configuration, consultez Configuration des outils pour les procédures détaillées.

   ```
   [profile UserDave]
   aws_access_key_id = access-key
   aws_secret_access_key = secret-access-key
   region = us-east-1
   ```

2. À l'invite de commande, entrez la AWS CLI commande suivante pour vérifier que Dave peut désormais obtenir une liste d'objets à partir du compte *amzn-s3-demo-bucket* appartenant au compte A. Notez que la commande spécifie le `UserDave` profil.

   ```
   aws s3 ls s3://amzn-s3-demo-bucket --profile UserDave
   ```

   Dave n'a aucune autre autorisation. Par conséquent, s'il essaie d'effectuer une autre opération (par exemple, la configuration `get-bucket-lifecycle` suivante), Amazon S3 indique que l'autorisation est refusée.

   ```
   aws s3api get-bucket-lifecycle-configuration --bucket amzn-s3-demo-bucket --profile
    UserDave
   ```

Tester les autorisations en utilisant AWS Tools for Windows PowerShell

1. Stockez les informations d'identification de Dave sous le nom `AccountBDave`.

   ```
   set-awscredentials -AccessKey AccessKeyID -SecretKey SecretAccessKey -storeas
    AccountBDave
   ```

2. Essayez la commande permettant de répertorier les compartiments.

   ```
   get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
   ```

   Dave n'a aucune autre autorisation. Par conséquent, s'il essaie d'effectuer une autre opération (par exemple, la commande `get-s3bucketlifecycleconfiguration` suivante), Amazon S3 indique que l'autorisation est refusée.

   ```
   get-s3bucketlifecycleconfiguration -BucketName amzn-s3-demo-bucket -
   StoredCredentials AccountBDave
   ```

Étape 3 : (Facultatif) essayer le refus explicite

Des autorisations peuvent vous être accordées à l'aide d'une liste de contrôle d'accès (ACL), d'une politique de compartiment ou d'une politique utilisateur. Toutefois, si un refus explicite est défini via une politique de compartiment ou une politique utilisateur, il prime sur toute autre autorisation. Pour le test, nous allons mettre à jour la politique de compartiment et refuser explicitement l'autorisation `s3:ListBucket` au compte B. Cette politique accorde également une autorisation `s3:ListBucket`. Cependant, le refus explicite prime, et le compte B ou les utilisateurs du compte B ne pourront pas afficher les objets dans *amzn-s3-demo-bucket*.

1. À l'aide des autorisations de l'utilisateur `AccountAadmin` dans le compte A, remplacez la politique de compartiment par les données suivantes.

   JSON

   ```
   {
      "Version": "2012-10-17",
      "Statement": [
         {
            "Sid": "Example permissions",
            "Effect": "Allow",
            "Principal": {
   ```

```
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:GetLifecycleConfiguration",
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      },
      {
         "Sid": "Deny permission",
         "Effect": "Deny",
         "Principal": {
            "AWS": "arn:aws:iam::AccountB-ID:root"
         },
         "Action": [
            "s3:ListBucket"
         ],
         "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket"
         ]
      }
   ]
}
```

2. Si vous essayez maintenant d'obtenir une liste des compartiments en utilisant les informations d'identification d'`AccountBadmin`, l'accès sera refusé.

   - À l'aide de AWS CLI, exécutez la commande suivante :

     ```
     aws s3 ls s3://amzn-s3-demo-bucket --profile AccountBadmin
     ```

   - À l'aide de AWS Tools for Windows PowerShell, exécutez la commande suivante :

     ```
     get-s3object -BucketName amzn-s3-demo-bucket -StoredCredentials AccountBDave
     ```

Étape 4 : nettoyer

1. Une fois le test terminé, vous pouvez procéder comme suit pour le nettoyage :

- Connectez-vous au AWS Management Console (AWS Management Console) à l'aide des informations d'identification du compte A, puis procédez comme suit :
  - Dans la console Amazon S3, supprimez la politique de compartiment attachée à *amzn-s3-demo-bucket*. Dans la page Properties du compartiment, supprimez la stratégie dans la section Permissions.
  - Si le compartiment a été créé pour cet exercice, supprimez les objets, puis le compartiment, dans la console Amazon S3.
  - Dans la console IAM, supprimez l'utilisateur `AccountAadmin`.
2. Connectez-vous à la console IAM en utilisant les informations d'identification du compte B. Supprimez l'utilisateur `AccountBadmin`. Pour step-by-step obtenir des instructions, consultez la section Suppression d'un utilisateur IAM dans le guide de l'utilisateur IAM.

Exemple 3 : propriétaire d'un compartiment accordant des autorisations sur des objets qu'il ne possède pas

> **Important**
>
> Il est préférable d'accorder des autorisations à des rôles IAM plutôt qu'à des utilisateurs individuels. Pour savoir comment procéder, consultez Fonctionnement des autorisations intercomptes et utilisation des rôles IAM.

Rubriques

- Étape 0 : vous préparer à suivre la procédure
- Étape 1 : Tâches du compte A
- Étape 2 : réaliser les tâches du compte B
- Étape 3 : tester les autorisations
- Étape 4 : nettoyer

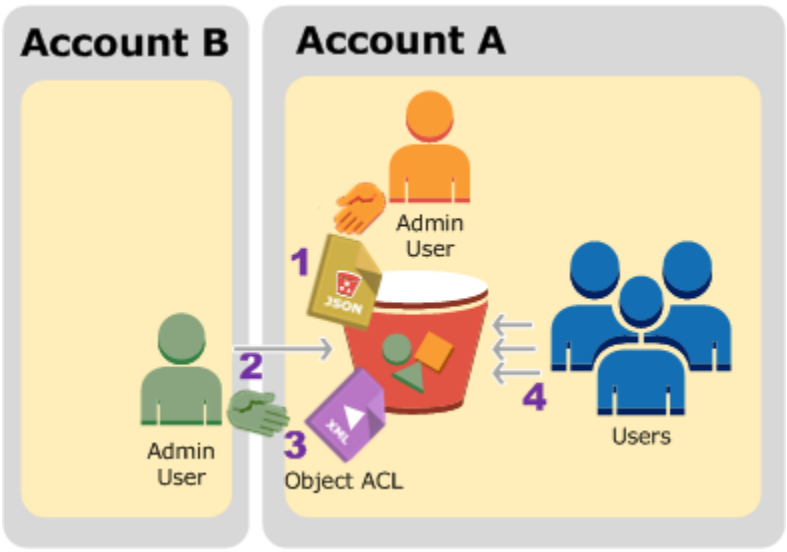
Le scénario de cet exemple met en scène un propriétaire de compartiment qui souhaite accorder l'autorisation d'accès à des objets, alors que tous les objets du compartiment ne lui appartiennent pas. Pour cet exemple, le propriétaire du compartiment essaie d'accorder une autorisation à des utilisateurs de son propre compte.

Le propriétaire d'un bucket peut autoriser d'autres Comptes AWS personnes à télécharger des objets. Par défaut, le propriétaire du compartiment ne possède pas d'objet écrit dans un compartiment par un autre Compte AWS. Les objets sont la propriété des comptes qui les écrivent dans un compartiment S3. Si le propriétaire du compartiment ne possède pas des objets dans le compartiment, le propriétaire des objets concernés doit d'abord accorder l'autorisation requise au propriétaire du compartiment à l'aide d'une liste de contrôle d'accès (ACL) d'objets. Le propriétaire du compartiment pourra ensuite accorder des autorisations à un objet dont il n'est pas propriétaire. Pour de plus amples informations, veuillez consulter Propriété du compartiment et de l'objet Amazon S3.

Si le propriétaire du compartiment applique le paramètre appliqué par le propriétaire du compartiment pour la propriété de l'objet S3 pour le compartiment, le propriétaire du compartiment possèdera tous les objets du compartiment, y compris les objets écrits par un autre Compte AWS. Cette approche résoudra le problème selon lequel les objets n'appartiennent pas au propriétaire du compartiment. Vous pouvez ensuite déléguer des autorisations à des utilisateurs de votre propre compte ou à d'autres Comptes AWS.

> **Note**
>
> La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès à ceux-ci exclusivement à l'aide de politiques de gestion des accès.
>
> La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Dans cet exemple, nous supposons que le propriétaire du compartiment n'a pas appliqué le paramètre appliqué par le propriétaire du compartiment pour la propriété de l'objet. Le propriétaire du compartiment délègue l'autorisation aux utilisateurs figurant dans son propre compte. Les étapes suivantes résument la procédure à suivre :



1. L'utilisateur administrateur du compte A attache une politique de compartiment contenant deux instructions.
   - Accorder une autorisation entre comptes au compte B pour charger des objets.
   - Autoriser un utilisateur dans son propre compte à accéder aux objets figurant dans le compartiment.
2. L'utilisateur administrateur du compte B charge des objets dans le compartiment appartenant au compte A.
3. L'administrateur du compte B met à jour la liste ACL d'objets en ajoutant une affectation qui donne au propriétaire du compartiment l'autorisation de contrôle total sur l'objet.
4. L'utilisateur figurant dans le compte A vérifie cela en accédant aux objets du compartiment, quel que soit leur propriétaire.

Pour cet exemple, vous avez besoin de deux comptes. Le tableau ci-dessous montre comment nous faisons référence à ces comptes et aux utilisateurs administrateurs dans ces comptes. Dans cette démonstration, vous n'utiliserez pas les autorisations d'utilisateur root du compte, conformément aux directives IAM recommandées. Pour plus d'informations, consultez Utilisation d'un utilisateur administrateur pour créer des ressources et accorder des autorisations. À la place, vous allez créer un administrateur dans chaque compte et utiliser ces autorisations pour créer des ressources et leur accorder des autorisations.

Compte AWS ID	Compte désigné comme	Administrateur du compte
1111-1111-1111	Compte A	AccountAadmin
2222-2222-2222	Compte B	AccountBadmin

Toutes les tâches de création d'utilisateurs et d'octroi d'autorisations sont effectuées dans la AWS Management Console. Pour vérifier les autorisations, la procédure pas à pas utilise les outils de ligne de commande AWS Command Line Interface (AWS CLI) et AWS Tools for Windows PowerShell vous n'avez donc pas besoin d'écrire de code.

Étape 0 : vous préparer à suivre la procédure

1. Assurez-vous d'en avoir deux Comptes AWS et d'avoir un administrateur pour chaque compte, comme indiqué dans le tableau de la section précédente.

   a. Inscrivez-vous pour un Compte AWS, si nécessaire.

   b. Utilisez les informations d'identification du compte A pour vous connecter à la console IAM et procédez comme suit pour créer un utilisateur administrateur :

      - Créez l'utilisateur **`AccountAadmin`** et notez ses informations d'identification de sécurité. Pour plus d'informations sur l'ajout d'utilisateurs, consultez Création d'un utilisateur IAM dans votre Compte AWS dans le Guide de l'utilisateur IAM.
      - Accordez des autorisations d'administrateur à AccountAadminen joignant une politique utilisateur qui donne un accès complet. Pour obtenir des instructions, consultez Gestion des politiques IAM dans le Guide de l'utilisateur IAM.
      - Dans le tableau de bord de la console IAM, notez l'URL de connexion d'utilisateur IAM. Les utilisateurs figurant dans ce compte doivent utiliser cette URL pour se connecter à la AWS Management Console. Pour plus d'informations, consultez Comment les utilisateurs se connectent à votre compte dans le Guide de l'utilisateur IAM.

   c. Répétez l'étape précédente en utilisant les informations d'identification du compte B et créez l'utilisateur administrateur **`AccountBadmin`**.

2. Configurez le AWS CLI ou les outils pour Windows PowerShell. Veillez à enregistrer les autorisations de l'administrateur comme suit :

   - Si vous utilisez le AWS CLI, créez deux profils, `AccountAadmin` et`AccountBadmin`, dans le fichier de configuration.

- Si vous utilisez les Outils pour Windows PowerShell, assurez-vous de stocker les informations d'identification de la session sous forme `AccountAadmin` et`AccountBadmin`.

Pour obtenir des instructions, veuillez consulter Configuration des outils pour les procédures détaillées.

Étape 1 : Tâches du compte A

Effectuez les opérations suivantes pour le compte A :

Étape 1.1 : vous connecter à la console

À l'aide de l'URL de connexion de l'utilisateur IAM pour le compte A, connectez-vous au compte en AWS Management Console tant qu'**`AccountAadmin`**utilisateur. Cet utilisateur créera un compartiment et y attachera une stratégie.

Étape 1.2 : créer un compartiment et un utilisateur, puis ajouter une politique de compartiment accordant des autorisations à l'utilisateur

1. Dans la console Amazon S3, créez un compartiment. Cet exercice suppose que le bucket a été créé dans l'est des États-Unis (Virginie du Nord) Région AWS et que son nom est*`amzn-s3-demo-bucket1`*.

   Pour obtenir des instructions, veuillez consulter Création d'un bucket à usage général.

2. Dans la console IAM, créez l'utilisateur **`Dave`**.

   Pour step-by-step obtenir des instructions, consultez la section Création d'utilisateurs IAM (console) dans le guide de l'utilisateur IAM.

3. Notez les informations d'identification de l'utilisateur Dave.

4. Dans la console Amazon S3, attachez la politique de compartiment suivante au compartiment *`amzn-s3-demo-bucket1`*. Pour obtenir des instructions, veuillez consulter Ajout d'une politique de compartiment à l'aide de la console Amazon S3. Suivez les étapes pour ajouter une politique de compartiment. Pour plus d'informations sur la recherche d'un compte IDs, consultez la section Trouver votre Compte AWS identifiant.

   Cette stratégie accorde au compte B les autorisations `s3:PutObject` et `s3:ListBucket`. Cette politique accorde également à l'utilisateur `Dave` l'autorisation `s3:GetObject`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
            "Action": [
                "s3:PutObject",
                "s3:ListBucket"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*",
                "arn:aws:s3:::amzn-s3-demo-bucket1"
            ]
        },
        {
            "Sid": "Statement3",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Dave"
            },
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1/*"
            ]
        }
    ]
}
```

Étape 2 : réaliser les tâches du compte B

Maintenant que le compte B est autorisé à effectuer des opérations sur le compartiment du compte A, l'administrateur du compte B procède comme suit :

- Charge un objet dans le compartiment du compte A
- Il ajoute une autorisation dans la liste ACL d'objets pour accorder le contrôle total au propriétaire du compartiment du compte A.

En utilisant le AWS CLI

1. À l'aide de la commande `put-object` AWS CLI , chargez un objet. Le paramètre `--body` de la commande identifie le fichier source à charger. Par exemple, si le fichier se trouve sur le lecteur `C:` d'un ordinateur Windows, spécifiez `c:\HappyFace.jpg`. Le paramètre `--key` fournit le nom de clé de l'objet.

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --body
 HappyFace.jpg --profile AccountBadmin
```

2. Ajoutez une affectation dans la liste ACL d'objets pour accorder au propriétaire du compartiment le contrôle total de l'objet. Pour découvrir comment trouver un ID d'utilisateur canonique, consultez Recherche de l'ID d'utilisateur canonique de votre Compte AWS dans le Guide de référence sur la gestion des comptes AWS .

```
aws s3api put-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --grant-
full-control id="AccountA-CanonicalUserID" --profile AccountBadmin
```

Utilisation des outils pour Windows PowerShell

1. À l'aide de la commande `Write-S3Object`, chargez un objet.

```
Write-S3Object -BucketName amzn-s3-demo-bucket1 -key HappyFace.jpg -file
 HappyFace.jpg -StoredCredentials AccountBadmin
```

2. Ajoutez une affectation dans la liste ACL d'objets pour accorder au propriétaire du compartiment le contrôle total de l'objet.

```
Set-S3ACL -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -CannedACLName
 "bucket-owner-full-control" -StoredCreden
```

Étape 3 : tester les autorisations

À présent, vérifiez que l'utilisateur Dave du compte A peut accéder à l'objet appartenant au compte B.

En utilisant le AWS CLI

1. Ajoutez les informations d'identification de l'utilisateur Dave au fichier de AWS CLI configuration et créez un nouveau profil,`UserDaveAccountA`. Pour de plus amples informations, veuillez consulter Configuration des outils pour les procédures détaillées.

   ```
   [profile UserDaveAccountA]
   aws_access_key_id = access-key
   aws_secret_access_key = secret-access-key
   region = us-east-1
   ```

2. Exécutez la commande CLI `get-object` pour télécharger `HappyFace.jpg`, puis enregistrez le fichier localement. Vous attribuez à l'utilisateur Dave des informations d'identification en ajoutant le paramètre `--profile`.

   ```
   aws s3api get-object --bucket amzn-s3-demo-bucket1 --key
    HappyFace.jpg Outputfile.jpg --profile UserDaveAccountA
   ```

Utilisation des outils pour Windows PowerShell

1. Stockez les AWS informations d'identification de l'utilisateur Dave`UserDaveAccountA`, comme dans le magasin permanent.

   ```
   Set-AWSCredentials -AccessKey UserDave-AccessKey -SecretKey UserDave-
   SecretAccessKey -storeas UserDaveAccountA
   ```

2. Exécutez la commande `Read-S3Object` pour télécharger `HappyFace.jpg`, puis enregistrez le fichier localement. Vous attribuez à l'utilisateur Dave des informations d'identification en ajoutant le paramètre `-StoredCredentials`.

   ```
   Read-S3Object -BucketName amzn-s3-demo-bucket1 -Key HappyFace.jpg -file
    HappyFace.jpg  -StoredCredentials UserDaveAccountA
   ```

Étape 4 : nettoyer

1. Une fois le test terminé, vous pouvez procéder comme suit pour le nettoyage :
   - Connectez-vous à la AWS Management Console en utilisant les informations d'identification du compte A, et procédez comme suit :
     - Dans la console Amazon S3, supprimez la politique de compartiment attachée à *amzn-s3-demo-bucket1*. Dans la page Properties du compartiment, supprimez la stratégie dans la section Permissions.
     - Si le compartiment a été créé pour cet exercice, supprimez les objets, puis le compartiment, dans la console Amazon S3.
     - Dans la console IAM, supprimez l'utilisateur AccountAadmin. Pour step-by-step obtenir des instructions, consultez la section Suppression d'un utilisateur IAM dans le guide de l'utilisateur IAM.
2. Connectez-vous à la AWS Management Console en utilisant les autorisations du compte B. Dans la console IAM, supprimez l'utilisateur AccountBadmin.

Exemple 4 : propriétaire d'un compartiment accordant des autorisations intercomptes à des objets qu'il ne possède pas

Rubriques

- Fonctionnement des autorisations intercomptes et utilisation des rôles IAM
- Étape 0 : vous préparer à suivre la procédure
- Étape 1 : réaliser les tâches du compte A
- Étape 2 : réaliser les tâches du compte B
- Étape 3 : réaliser les tâches du compte C
- Étape 4 : nettoyer
- Ressources connexes

Dans cet exemple de scénario, vous êtes propriétaire d'un bucket et vous avez autorisé d'autres utilisateurs Comptes AWS à télécharger des objets. Si vous avez appliqué le paramètre appliqué par le propriétaire du compartiment pour la propriété de l'objet S3 pour le compartiment, vous posséderez tous les objets du compartiment, y compris les objets écrits par un autre Compte AWS. Cette approche résoudra le problème selon lequel les objets n'appartiennent pas au propriétaire

du compartiment, à savoir vous-même. Vous pouvez ensuite déléguer des autorisations à des utilisateurs de votre propre compte ou à d'autres Comptes AWS. Supposons que le paramètre appliqué par le propriétaire du compartiment pour la propriété de l'objet S3 ne soit pas activé. C'est pourquoi le compartiment peut avoir des objets détenus par d'autres Comptes AWS .

A présent, admettons qu'en tant que propriétaire du compartiment, vous devez accorder des autorisations entre comptes sur des objets, quel que soit le propriétaire, à un utilisateur d'un autre compte. Par exemple, cet utilisateur peut être une application de facturation qui a besoin d'accéder aux métadonnées d'objet. Deux problèmes majeurs se posent :

- Le propriétaire du compartiment n'a aucune autorisation sur ces objets créés par d'autres Comptes AWS. Pour que le propriétaire du compartiment accorde les autorisations sur des objets qu'il ne possède pas, le propriétaire des objets concernés doit tout d'abord accorder l'autorisation requise au propriétaire du compartiment. Le propriétaire des objets correspond au Compte AWS qui a créé ces objets. Le propriétaire du compartiment peut alors déléguer ces autorisations.
- Le compte du propriétaire du compartiment peut déléguer des autorisations aux utilisateurs associés à son propre compte (voir Exemple 3 : propriétaire d'un compartiment accordant des autorisations sur des objets qu'il ne possède pas). Toutefois, le compte du propriétaire du compartiment ne peut pas déléguer d'autorisations à d'autres personnes, Comptes AWS car la délégation entre comptes n'est pas prise en charge.

Dans ce scénario, le propriétaire du compartiment peut créer un rôle AWS Identity and Access Management (IAM) autorisé à accéder aux objets. Ensuite, le propriétaire du compartiment peut accorder une autre Compte AWS autorisation pour assumer le rôle, lui permettant ainsi temporairement d'accéder aux objets du compartiment.

> **Note**
>
> La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès à ceux-ci exclusivement à l'aide de politiques de gestion des accès.
>
> La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances

exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Fonctionnement des autorisations intercomptes et utilisation des rôles IAM

Les rôles IAM permettent à plusieurs scénarios de déléguer l'accès aux ressources, et l'accès intercompte est l'un des scénarios clés. Dans cet exemple, le propriétaire du compartiment, le compte A, utilise un rôle IAM pour déléguer temporairement l'accès aux objets entre comptes aux utilisateurs d'un autre Compte AWS, le compte C. Chaque rôle IAM que vous créez est associé aux deux politiques suivantes :

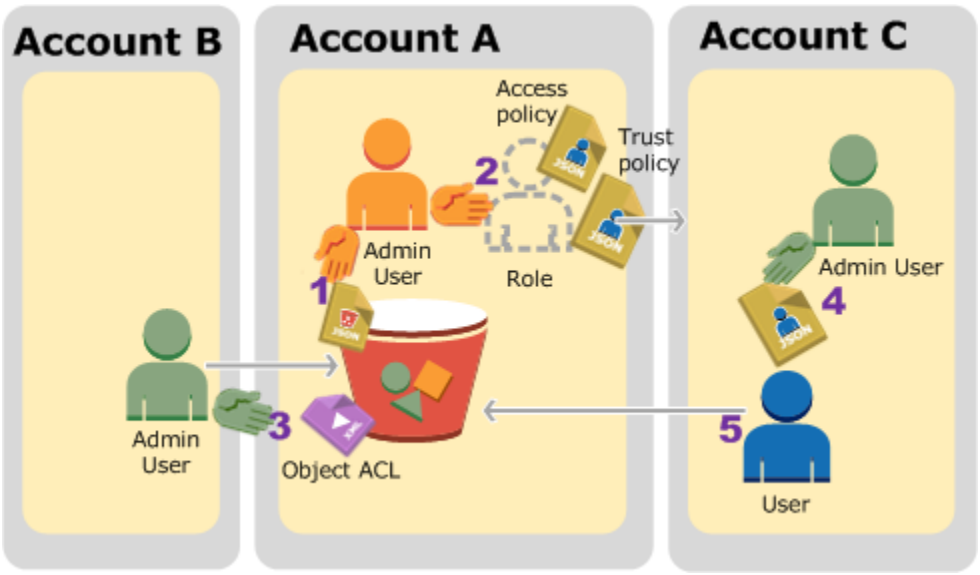
- Une politique de confiance identifiant une autre Compte AWS personne qui peut assumer le rôle.
- Une stratégie d'accès qui définit les autorisations : par exemple, `s3:GetObject`, accordées lorsqu'une personne assume le rôle. Pour obtenir une liste d'autorisations que vous pouvez spécifier dans une stratégie, consultez Actions de politique pour Amazon S3.

La Compte AWS personne identifiée dans la politique de confiance accorde ensuite à son utilisateur l'autorisation d'assumer le rôle. L'utilisateur peut ensuite procéder comme suit pour accéder aux objets :

- Assumez le rôle et, en réponse, obtenir des autorisations de sécurité temporaires.
- Accédez aux objets dans le compartiment grâce aux autorisations de sécurité temporaires.

Pour plus d'informations sur les rôles IAM, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

Les étapes suivantes résument la procédure à suivre :



1. L'utilisateur administrateur du Compte A attache une politique de compartiment en accordant au Compte B l'autorisation conditionnelle de charger des objets.
2. L'administrateur du Compte A crée un rôle IAM, en instaurant la confiance avec le Compte C, afin que les utilisateurs de ce compte puissent accéder au Compte A. La stratégie d'accès attachée au rôle limite les actions de l'utilisateur du Compte C lorsque ce dernier accède au Compte A.
3. L'administrateur du compte B charge un objet dans le compartiment détenu par le Compte A, en accordant l'autorisation de contrôle total au propriétaire du compartiment.
4. L'administrateur du Compte C crée un utilisateur et attache une stratégie d'utilisateur qui permet à l'utilisateur d'assumer le rôle.
5. L'utilisateur du Compte C assume tout d'abord le rôle, qui lui renvoie les autorisations de sécurité temporaires. Grâce à ces autorisations, l'utilisateur accède ensuite aux objets du compartiment.

Pour cet exemple, vous avez besoin de trois comptes. Le tableau ci-dessous montre comment nous faisons référence à ces comptes et aux utilisateurs administrateurs dans ces comptes. Conformément aux directives IAM (voir Utilisation d'un utilisateur administrateur pour créer des ressources et accorder des autorisations), nous n'utilisons pas les informations d'identification Utilisateur racine d'un compte AWS dans cette procédure détaillée. A la place, vous créez un utilisateur administrateur dans chaque compte et utilisez ces autorisations pour créer des ressources et leur accorder des autorisations.

Compte AWS ID	Compte désigné comme	Utilisateur administrateur du compte
1111-1111-1111	Compte A	AccountAadmin
2222-2222-2222	Compte B	AccountBadmin
3333-3333-3333	Compte C	AccountCadmin

Étape 0 : vous préparer à suivre la procédure

> **Note**
>
> Vous pouvez ouvrir un éditeur de texte et écrire certaines informations à mesure que vous parcourez les étapes. Vous aurez notamment besoin d'un compte IDs, d'un utilisateur canonique IDs, d'une connexion utilisateur IAM URLs pour chaque compte pour vous connecter à la console, ainsi que des noms de ressources Amazon (ARNs) des utilisateurs IAM et des rôles.

1. Assurez-vous que vous en avez trois Comptes AWS et que chaque compte possède un utilisateur administrateur, comme indiqué dans le tableau de la section précédente.

   a. Inscrivez-vous Comptes AWS, au besoin. Nous appelons ces comptes : Compte A, Compte B et Compte C.

   b. Utilisez les informations d'identification du compte A pour vous connecter à la console IAM et procédez comme suit pour créer un utilisateur administrateur :

      - Créez l'utilisateur **`AccountAadmin`** et notez ses informations d'identification. Pour plus d'informations sur l'ajout d'utilisateurs, consultez Création d'un utilisateur IAM dans votre Compte AWS dans le Guide de l'utilisateur IAM.
      - Accordez des privilèges d'administrateur à AccountAadminen joignant une politique utilisateur donnant un accès complet. Pour obtenir des instructions, consultez Gestion des politiques IAM dans le Guide de l'utilisateur IAM.
      - Dans le tableau de bord de la console IAM, notez l'URL de connexion d'utilisateur IAM. Les utilisateurs figurant dans ce compte doivent utiliser cette URL pour se connecter

à la AWS Management Console. Pour plus d'informations, voir Se connecter en AWS Management Console tant qu'utilisateur IAM dans le guide de l'utilisateur IAM.

c. Répétez l'étape précédente pour créer les utilisateurs administrateur dans le Compte B et le Compte C.

2. Pour le compte C, notez l'ID d'utilisateur canonique.

   Lorsque vous créez un rôle IAM dans le Compte A, la stratégie d'approbation accorde au Compte C l'autorisation d'assumer le rôle en spécifiant l'ID de compte. Vous pouvez trouver les informations de compte comme suit :

   a. Utilisez votre Compte AWS identifiant ou alias de compte, votre nom d'utilisateur IAM et votre mot de passe pour vous connecter à la console Amazon S3.

   b. Choisissez le nom d'un compartiment Amazon S3 pour afficher les détails concernant ce compartiment.

   c. Sélectionnez l'onglet Permissions (Autorisations), puis Access Control List (Liste de contrôle d'accès).

   d. Dans la section Accès à votre Compte AWS, dans la colonne Account (Compte) figure un identifiant long tel que `c1daexampleaaf850ea79cf0430f33d72579fd1611c97f7ded193374c0b163b6`. Ceci est votre ID d'utilisateur canonique.

3. Lorsque vous créez une politique de compartiment, vous avez besoin des informations suivantes. Notez ces valeurs :

   - ID d'utilisateur canonique du Compte A – Lorsque l'administrateur du Compte A accorde une autorisation conditionnelle de téléchargement d'objet à l'administrateur du Compte B, la condition spécifie l'ID d'utilisateur canonique de l'utilisateur du Compte A qui doit obtenir le contrôle total des objets.

     > **Note**
     >
     > Le concept d'ID d'utilisateur canonique est propre à Amazon S3. Il s'agit d'une version cryptée de 64 caractères de l'ID de compte.

   - ARN de l'utilisateur pour l'administrateur du compte B : vous trouverez l'ARN de l'utilisateur dans la console IAM. Pour ce faire, sélectionnez l'utilisateur et trouvez son ARN dans l'onglet Récapitulatif.

Dans la politique de compartiment, vous accordez à `AccountBadmin` l'autorisation de charger des objets et vous spécifiez l'utilisateur grâce à l'ARN. Voici un exemple de valeur ARN :

```
arn:aws:iam::AccountB-ID:user/AccountBadmin
```

4. Configurez le AWS Command Line Interface (CLI) ou le AWS Tools for Windows PowerShell. Assurez-vous d'enregistrer les autorisations de l'utilisateur administrateur comme suit :

   - Si vous utilisez le AWS CLI, créez des profils`AccountBadmin`, `AccountAadmin` et dans le fichier de configuration.
   - Si vous utilisez le AWS Tools for Windows PowerShell, assurez-vous de stocker les informations d'identification de la session sous forme `AccountAadmin` et`AccountBadmin`.

   Pour obtenir des instructions, veuillez consulter Configuration des outils pour les procédures détaillées.

Étape 1 : réaliser les tâches du compte A

Dans cet exemple, le Compte A est le propriétaire du compartiment. L'utilisateur AccountAadmin du compte A effectuera donc ce qui suit :

- Créez un compartiment.
- Attachez la politique de compartiment suivante en accordant à l'administrateur du compte B l'autorisation conditionnelle de charger des objets.
- Créez un rôle IAM en accordant l'autorisation au Compte C d'endosser ce rôle afin qu'il puisse accéder aux objets du compartiment.

Étape 1.1 : Connectez-vous au AWS Management Console

À l'aide de l'URL de connexion de l'utilisateur IAM pour le compte A, connectez-vous d'abord au compte en AWS Management Console tant qu'**`AccountAadmin`**utilisateur. Cet utilisateur créera un compartiment et y attachera une stratégie.

Étape 1.2 : créer un compartiment et attacher une politique de compartiment

Dans la console Amazon S3, procédez comme suit :

1. Créez un compartiment. Cet exercice assume que le nom du compartiment est *amzn-s3-demo-bucket1*.

   Pour obtenir des instructions, veuillez consulter Création d'un bucket à usage général.

2. Attachez la politique de compartiment suivante. Cette politique accorde à l'administrateur du compte B l'autorisation conditionnelle de charger des objets.

   Mettez à jour la politique en fournissant vos propres valeurs pour *amzn-s3-demo-bucket1*, *AccountB-ID* et *CanonicalUserId-of-AWSaccountA-BucketOwner*.

   JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "111",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
        },
        {
            "Sid": "112",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=CanonicalUserId-of-
AWSaccountA-BucketOwner"
                }
            }
        }
    ]
}
```

Étape 1.3 : créer un rôle IAM pour accorder au compte C un accès intercompte au compte A

Dans la console IAM, créez un rôle IAM (**`examplerole`**) qui accorde l'autorisation au Compte C d'endosser ce rôle. Veillez à être toujours connecté comme administrateur du compte A, car le rôle doit être créé dans ce compte.

1. Avant de créer le rôle, préparez la politique gérée qui définit les autorisations qu'exige le rôle. Vous attachez cette politique au rôle dans une étape ultérieure.

   a. Dans le volet de navigation de gauche, sélectionnez Politiques, puis Créer une politique.

   b. En regard de Create Your Own Policy (Créez votre politique), choisissez Select (Sélectionner).

   c. Saisissez **`access-accountA-bucket`** dans le champ Policy Name.

   d. Copiez la stratégie d'accès suivante et collez-la dans le champ Policy Document. La stratégie d'accès accorde l'autorisation `s3:GetObject` au rôle. Des lors, quand l'utilisateur du Compte C assumera ce rôle, il pourra uniquement exécuter l'opération `s3:GetObject`.

      JSON

      ```
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Effect": "Allow",
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*"
          }
        ]
      }
      ```

   e. Choisissez Create Policy (Créer une politique).

      La nouvelle politique apparaît dans la liste des politiques gérées.

2. Dans le volet de navigation de gauche, sélectionnez Rôles, puis Créer un rôle.
3. Sous Sélectionner le type de rôle, sélectionnez Rôle pour l'accès entre comptes, puis cliquez sur le bouton Sélectionner à côté de Fournir un accès entre les Comptes AWS vôtres.
4. Saisissez l'ID de compte du Compte C.

Pour cette procédure détaillée, vous n'avez pas besoin d'exiger des utilisateurs qu'ils aient l'authentification multifactorielle (MFA) pour endosser le rôle. Ne cochez donc pas cette option.

5. Cliquez sur Étape suivante pour configurer les autorisations associées au rôle.
6. Cochez la case située à côté de la politique access-accountA-bucket que vous avez créée, puis choisissez Étape suivante.

   La page de révision apparaît pour que vous confirmiez les paramètres pour le rôle avant qu'il ne soit créé. Sur cette page, il est très important que vous notiez le lien que vous pouvez envoyer aux utilisateurs qui ont besoin d'utiliser ce rôle. Les utilisateurs qui cliquent sur le lien accèdent directement à la page Changer de rôle dont les champs ID de compte et Nom du rôle sont déjà remplis. Vous pourrez également consulter ce lien ultérieurement sur la page Résumé du rôle pour n'importe quel rôle intercompte.
7. Saisissez le nom de rôle `examplerole`, puis choisissez Étape suivante.
8. Après avoir procédé à la vérification du rôle, sélectionnez Créer un rôle.

   Le rôle `examplerole` est affiché dans la liste des rôles.
9. Sélectionnez le nom de rôle `examplerole`.
10. Sélectionnez l'onglet Trust Relationships.
11. Cliquez sur Afficher le document de stratégie et vérifiez que la politique d'approbation affichée correspond à la politique suivante.

    La stratégie d'approbation suivante instaure la confiance avec le Compte C, en lui permettant d'exécuter l'action `sts:AssumeRole`. Pour plus d'informations, consultez AssumeRole dans la Référence d'API AWS Security Token Service .

    JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:root"
            },
```

```
            "Action": "sts:AssumeRole"
        }
    ]
}
```

12. Notez l'Amazon Resource Name (ARN) du rôle `examplerole` que vous avez créé.

    Dans les étapes suivantes, vous attachez une stratégie d'utilisateur pour permettre un utilisateur IAM d'assumer ce rôle et vous identifiez le rôle par la valeur ARN.

Étape 2 : réaliser les tâches du compte B

L'exemple de compartiment détenu par le compte A a besoin d'objets détenus par d'autres comptes. Dans cette étape, l'administrateur du Compte B charge un objet grâce aux outils de ligne de commande.

- À l'aide de la `put-object` AWS CLI commande, chargez un objet vers*amzn-s3-demo-bucket1*.

  ```
  aws s3api put-object --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
  body HappyFace.jpg --grant-full-control id="canonicalUserId-ofTheBucket0wner" --
  profile AccountBadmin
  ```

  Remarques :

  - Le paramètre `--Profile` spécifie le profil `AccountBadmin`, afin que l'objet soit détenu par le compte B.
  - Le paramètre `grant-full-control` accorde au propriétaire du compartiment l'autorisation de contrôle total sur l'objet comme l'exige la politique de compartiment.
  - Le paramètre `--body` identifie le fichier source à charger. Par exemple, si le fichier est sur le lecteur C: d'un ordinateur Windows, vous spécifiez `c:\HappyFace.jpg`.

Étape 3 : réaliser les tâches du compte C

Dans les étapes précédentes, le Compte A a déjà créé un rôle, `examplerole`, instaurant la confiance avec le Compte C. Cela permet aux utilisateurs du Compte C d'accéder au Compte A. Dans cette étape, l'administrateur du Compte C crée un utilisateur (Dave) et lui délègue l'autorisation `sts:AssumeRole` reçue par le Compte A. Cela permet à Dave d'endosser le rôle `examplerole` et d'accéder temporairement au Compte A. La stratégie d'accès que le Compte A a associée au rôle

limite les actions de Dave lorsqu'il accède au Compte A, notamment l'obtention d'objets dans *amzn-s3-demo-bucket1*.

Étape 3.1 : créer un utilisateur dans le compte C et déléguer l'autorisation d'endosser le rôle examplerole

1. À l'aide de l'URL de connexion utilisateur IAM pour le compte C, connectez-vous d'abord au compte en AWS Management Console tant qu'**AccountCadmin**utilisateur.

2. Dans la console IAM, créez un utilisateur, Dave.

   Pour step-by-step obtenir des instructions, consultez la section Création d'utilisateurs IAM (AWS Management Console) dans le guide de l'utilisateur IAM.
3. Notez les informations d'identification de Dave. Dave a besoin de ces informations d'identification pour assumer le rôle `examplerole`.
4. Créez une politique intégrée pour l'utilisateur IAM Dave, afin de lui déléguer l'autorisation `sts:AssumeRole` au niveau du rôle `examplerole` dans le Compte A.

   a. Dans le volet de navigation de gauche, choisissez Utilisateurs.
   b. Choisissez le nom d'utilisateur Dave.
   c. Dans la page des détails de l'utilisateur, sélectionnez l'onglet Autorisations et développez la section Politiques en ligne.
   d. Choisissez click here (ou Create User Policy).
   e. Choisissez Custom Policy, puis Select.
   f. Saisissez un nom pour la stratégie dans le champ Policy Name.
   g. Copiez la stratégie suivante dans le champ Policy Document.

      Pour mettre à jour la politique, fournissez l'*AccountA-ID*.

      JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
```

```
            ],
            "Resource": "arn:aws:iam::111122223333:role/examplerole"
        }
    ]
}
```

h. Choisissez Apply Policy (Appliquer la stratégie).

5. Enregistrez les informations d'identification de Dave dans le fichier de configuration du AWS CLI en ajoutant un autre profil,`AccountCDave`.

```
[profile AccountCDave]
aws_access_key_id = UserDaveAccessKeyID
aws_secret_access_key = UserDaveSecretAccessKey
region = us-west-2
```

Étape 3.2 : endosser le rôle (examplerole) et accéder à des objets

A présent, Dave peut accéder aux objets du compartiment détenu par le Compte A comme suit :

- Dave assume tout d'abord le rôle `examplerole` grâce à ses propres informations d'identification. Cela renvoie des autorisations temporaires.
- Grâce aux autorisations, Dave accède ensuite aux objets du compartiment du Compte A.

1. À l'invite de commande, exécutez la AWS CLI `assume-role` commande suivante à l'aide du `AccountCDave` profil.

   Vous devez mettre à jour la valeur ARN dans la commande en fournissant l'*AccountA-ID* dans lequel le rôle `examplerole` est défini.

```
aws sts assume-role --role-arn arn:aws:iam::AccountA-ID:role/examplerole --profile
 AccountCDave --role-session-name test
```

   En réponse, AWS Security Token Service (AWS STS) renvoie des informations de sécurité temporaires (ID de clé d'accès, clé d'accès secrète et jeton de session).

2. Enregistrez les informations de sécurité temporaires dans le fichier de AWS CLI configuration situé sous le `TempCred` profil.

```
[profile TempCred]
```

```
aws_access_key_id = temp-access-key-ID
aws_secret_access_key = temp-secret-access-key
aws_session_token = session-token
region = us-west-2
```

3. À l'invite de commande, exécutez la AWS CLI commande suivante pour accéder aux objets à l'aide des informations d'identification temporaires. Par exemple, la commande spécifie l'API d'objet HEAD pour récupérer les métadonnées d'objet pour l'objet `HappyFace.jpg`.

```
aws s3api get-object --bucket amzn-s3-demo-bucket1 --
key HappyFace.jpg SaveFileAs.jpg --profile TempCred
```

Etant donné que la stratégie d'accès attachée au rôle `examplerole` autorise les actions, Amazon S3 traite la demande. Vous pouvez essayer n'importe quelle autre action sur n'importe quel objet du compartiment.

Si vous essayez une autre action (par exemple, `get-object-acl`), l'autorisation est refusée, car le rôle ne permet pas cette action.

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket1 --key HappyFace.jpg --
profile TempCred
```

Nous avons utilisé Dave pour assumer le rôle et accéder à l'objet grâce à des autorisations temporaires. Il peut s'agir également d'une application dans le Compte C qui accède aux objets dans le compartiment *amzn-s3-demo-bucket1*. L'application peut obtenir des informations d'identification de sécurité temporaires, et le Compte C peut déléguer l'autorisation d'application pour assumer le rôle `examplerole`.

Étape 4 : nettoyer

1. Une fois le test terminé, vous pouvez procéder comme suit pour le nettoyage :

   - Connectez-vous à la AWS Management Console en utilisant les informations d'identification du compte A, et procédez comme suit :

     - Dans la console Amazon S3, supprimez la politique de compartiment attachée à *amzn-s3-demo-bucket1*. Dans la page Properties du compartiment, supprimez la stratégie dans la section Permissions.

- Si le compartiment a été créé pour cet exercice, supprimez les objets, puis le compartiment, dans la console Amazon S3.
- Dans la console IAM, supprimez le `examplerole` que vous avez créé dans le compte A. Pour step-by-step obtenir des instructions, voir Supprimer un utilisateur IAM dans le guide de l'utilisateur IAM.
- Dans la console IAM, supprimez l'utilisateur AccountAadmin.

2. Connectez-vous à la console IAM en utilisant les informations d'identification du compte B. Supprimez l'utilisateur AccountBadmin.
3. Connectez-vous à la console IAM en utilisant les informations d'identification du compte C. Supprimer AccountCadminet l'utilisateur Dave.

Ressources connexes

Pour plus d'informations relatives à cette procédure détaillée, consultez les ressources suivantes dans le Guide de l'utilisateur IAM :

- Création d'un rôle pour la délégation d'autorisations à un utilisateur IAM
- Tutoriel : Déléguer l'accès à Comptes AWS l'aide de rôles IAM
- Gestion des politiques IAM

Utilisation des rôles liés à un service pour Amazon S3 Storage Lens

Pour utiliser Amazon S3 Storage Lens afin de collecter et agréger des mesures sur tous vos comptes dans les AWS Organizations, vous devez d'abord vous assurer que S3 Storage Lens dispose d'un accès fiable activé par le compte de gestion de votre organisation. S3 Storage Lens crée un rôle lié à un service (SLR) pour lui permettre d'obtenir la liste des Comptes AWS membres de votre organisation. Cette liste de comptes est utilisée par S3 Storage Lens pour collecter des mesures des ressources S3 dans tous les comptes membres lorsque le tableau de bord ou les configurations de S3 Storage Lens sont créés ou mis à jour.

Amazon S3 Storage Lens utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement au S3 Storage Lens. Les rôles liés au service sont prédéfinis par S3 Storage Lens et incluent toutes les autorisations dont le service a besoin pour appeler d'autres personnes en votre Services AWS nom.

Un rôle lié à un service simplifie la configuration de S3 Storage Lens car vous n'avez pas besoin d'ajouter manuellement les autorisations requises. S3 Storage Lens définit les autorisations de ses rôles liés à un service et, sauf définition contraire, seul S3 Storage Lens peut endosser ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer le rôle lié à un service uniquement après avoir supprimé les ressources connexes. Vos ressources relatives au S3 Storage Lens sont ainsi protégées, car vous ne pouvez pas accidentellement supprimer les autorisations d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés à un service, consultez AWS services that work with IAM (Services AWS fonctionnant avec IAM) et recherchez les services avec un Yes (Oui) dans la colonne Service-Linked Role (Rôle lié à un service). Choisissez un Oui ayant un lien permettant de consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle liées au service pour Amazon S3 Storage Lens

S3 Storage Lens utilise le rôle lié au service nommé AWSServiceRoleForS3 StorageLens. Cela permet d'accéder aux AWS services et aux ressources utilisés ou gérés par S3 Storage Lens. Cela permet à S3 Storage Lens d'accéder aux AWS Organizations ressources en votre nom.

Le rôle lié à un service S3 Storage Lens approuve le service suivant sur le stockage de votre organisation :

- `storage-lens.s3.amazonaws.com`

La stratégie d'autorisations liée au rôle permet au S3 Storage Lens de réaliser les actions suivantes :

- `organizations:DescribeOrganization`

  `organizations:ListAccounts`

  `organizations:ListAWSServiceAccessForOrganization`

  `organizations:ListDelegatedAdministrators`

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Autorisations de rôles liés à un service dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour S3 Storage Lens

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous effectuez l'une des tâches suivantes alors que vous êtes connecté aux comptes AWS Organizations de gestion ou d'administrateur délégué, S3 Storage Lens crée le rôle lié au service pour vous :

- Créez une configuration de tableau de bord S3 Storage Lens pour votre organisation dans la console Amazon S3.
- PUTune configuration S3 Storage Lens pour votre organisation à l'aide de l'API REST, AWS CLI et SDKs.

> **Note**
>
> S3 Storage Lens prend en charge un maximum de cinq administrateurs délégués par organisation.

Si vous supprimez ce rôle lié à un service, les actions précédentes le recréeront si nécessaire.

Exemple de stratégie pour un rôle lié à un service de S3 Storage Lens

Example Stratégie d'autorisations pour le rôle lié à un service de S3 Storage Lens

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AwsOrgsAccess",
            "Effect": "Allow",
            "Action": [
                "organizations:DescribeOrganization",
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators"
            ],
            "Resource": [
                "*"
            ]
```

```
        }
    ]
}
```

Modification d'un rôle lié à un service pour Amazon S3 Storage Lens

S3 Storage Lens ne vous permet pas de modifier le rôle lié à un service AWSServiceRoleForS3StorageLens. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au 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 IAM Guide de l'utilisateur.

Suppression d'un rôle lié à un service pour Amazon S3 Storage Lens

Si vous n'utilisez plus le 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 Amazon S3 Storage Lens 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 le, AWSServiceRoleForS3StorageLens vous devez supprimer toutes les configurations S3 Storage Lens présentes au niveau de l'organisation à Régions AWS l'aide des comptes de AWS Organizations gestion ou d'administrateur délégué.

Les ressources sont des configurations de S3 Storage Lens au niveau de l'organisation. Utilisez S3 Storage Lens pour nettoyer les ressources, puis utilisez la console IAM, la CLI, l'API REST ou le AWS SDK pour supprimer le rôle.

Dans les API REST, et AWS CLI SDKs, les configurations S3 Storage Lens peuvent être découvertes `ListStorageLensConfigurations` dans toutes les régions dans lesquelles votre organisation a créé des configurations S3 Storage Lens. Utilisez l'action `DeleteStorageLensConfiguration` pour supprimer ces configurations afin de pouvoir ensuite supprimer le rôle.

> **Note**
>
> Pour supprimer le rôle lié au service, vous devez supprimer toutes les configurations de S3 Storage Lens au niveau de l'organisation dans toutes les Régions où elles existent.

Pour supprimer les ressources Amazon S3 Storage Lens utilisées par le rôle lié au service AWSServiceRoleForS3StorageLens

1. Pour obtenir une liste des configurations au niveau de votre organisation, vous devez utiliser `ListStorageLensConfigurations` dans chaque région où vous disposez de configurations S3 Storage Lens. Cette liste peut également être obtenue à partir de la console Amazon S3.
2. Supprimez ces configurations des points de terminaison régionaux appropriés en invoquant l'appel d'API `DeleteStorageLensConfiguration` ou à l'aide de la console Amazon S3.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Après avoir supprimé les configurations, supprimez le AWSServiceRoleForS3StorageLens SLR de la console IAM, en appelant l'API IAM ou en utilisant `DeleteServiceLinkedRole` le SDK. AWS CLI AWS Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions supportées pour les rôles liés à un service de S3 Storage Lens

S3 Storage Lens prend en charge l'utilisation de rôles liés au service partout Régions AWS où le service est disponible. Pour plus d'informations, consultez Régions et points de terminaison Amazon S3.

Résolution des problèmes d'identité et d'accès Amazon S3

Utilisez les informations suivantes pour identifier et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec Amazon S3 et IAM.

Rubriques

- J'ai reçu un message d'erreur pour cause d'accès refusé
- Je ne suis pas autorisé à effectuer une action dans Amazon S3
- Je ne suis pas autorisé à effectuer iam : PassRole

- Je souhaite autoriser des personnes extérieures Compte AWS à moi à accéder à mes ressources Amazon S3
- Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3

J'ai reçu un message d'erreur pour cause d'accès refusé

Vérifiez qu'il n'existe aucune instruction `Deny` explicite à l'encontre du demandeur auquel vous essayez d'accorder des autorisations, que ce soit dans la politique de compartiment ou dans la politique basée sur l'identité.

Pour obtenir des informations détaillées sur la résolution des erreurs d'accès refusé, consultez Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3.

Je ne suis pas autorisé à effectuer une action dans Amazon S3

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 `s3:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 s3: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 `s3:`*`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 Amazon S3.

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, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Amazon S3. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer 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 Compte AWS à moi à accéder à mes ressources Amazon S3

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 (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Amazon S3 est compatible avec ces fonctionnalités, consultez Fonctionnement d'Amazon S3 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.

Résolution des erreurs d'accès refusé (403 Forbidden) dans Amazon S3

Des erreurs d'accès refusé (HTTP`403 Forbidden`) apparaissent en cas de refus AWS explicite ou implicite d'une demande d'autorisation.

- Un refus explicite se produit lorsqu'une politique contient une `Deny` déclaration pour une AWS action spécifique.
- Un refus implicite se produit lorsqu'il n'y a ni d'instruction `Deny` applicable ni d'instruction `Allow` applicable.

Étant donné qu'une politique AWS Identity and Access Management (IAM) refuse implicitement un principal IAM par défaut, elle doit explicitement autoriser le principal à effectuer une action. Dans le cas contraire, la politique refuse implicitement l'accès. Pour plus d'informations, consultez Différence entre les refus explicites et implicites dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la logique d'évaluation des politiques qui détermine si une demande d'accès est autorisée ou refusée, consultez Logique d'évaluation des politiques dans le Guide de l'utilisateur d'IAM.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Les rubriques suivantes décrivent les causes les plus courantes des erreurs d'accès refusé dans Amazon S3.

> **Note**
>
> En cas d'erreur d'accès refusé (HTTP`403 Forbidden`), Amazon S3 ne facture pas le propriétaire du compartiment lorsque la demande est initiée en dehors du AWS compte individuel du propriétaire du compartiment ou de l' AWS organisation du propriétaire du compartiment.

Rubriques

- Exemples de messages de refus d'accès et étapes à suivre pour les résoudre

- Politiques de compartiment et politiques IAM
- Paramètres des listes de contrôle d'accès d'Amazon S3
- Paramètres de blocage de l'accès public S3
- Paramètres du chiffrement Amazon S3
- Paramètres de verrouillage des objets S3
- Politiques de point de terminaison d'un VPC
- AWS Organizations politiques
- CloudFront accès à la distribution
- Paramètres du point d'accès
- Ressources supplémentaires

> **Note**
>
> Si vous essayez de résoudre un problème d'autorisation, commencez par la section the section called "Exemples de messages de refus d'accès et étapes à suivre pour les résoudre", puis passez à la section ???. Assurez-vous également de suivre les instructions figurant dansthe section called "Conseils pour vérifier les autorisations".

Exemples de messages de refus d'accès et étapes à suivre pour les résoudre

> **Important**
>
> Dans les semaines à venir, à compter du 16 juin 2025, Amazon S3 commencera à fournir des messages d'erreur de refus d'accès améliorés pour les demandes adressées aux ressources des comptes de la même organisation dans AWS Organizations. Ces messages seront disponibles dans toutes les régions Régions AWS, y compris dans les régions AWS GovCloud (US) Regions et en Chine.

Amazon S3 inclut désormais un contexte supplémentaire dans les erreurs de refus d'accès (HTTP`403 Forbidden`) pour les demandes adressées aux ressources de la même Compte AWS ou de la même organisation dans AWS Organizations. Ce nouveau contexte inclut le type de politique qui a refusé l'accès, le motif du refus et les informations sur l'utilisateur ou le rôle IAM qui a demandé l'accès à la ressource.

Ce contexte supplémentaire vous aide à résoudre les problèmes d'accès, à identifier la cause première des erreurs de refus d'accès et à corriger les contrôles d'accès incorrects en mettant à jour les politiques pertinentes. Ce contexte supplémentaire est également disponible dans les AWS CloudTrail journaux. Les messages d'erreur de refus d'accès améliorés pour les demandes concernant le même compte ou la même organisation sont désormais disponibles dans toutes les régions Régions AWS, y compris en Chine et AWS GovCloud (US) Regions en Chine.

La plupart des messages d'erreur d'accès refusé se présentent sous le format `User` *`user-arn`* `is not authorized to perform` *`action`* `on "`*`resource-arn`*`" because` *`context`*. Dans cet exemple, *`user-arn`* est l'Amazon Resource Name (ARN) de l'utilisateur qui ne reçoit pas d'accès, *`action`* est l'action de service refusée par la politique, et *`resource-arn`* est l'ARN de la ressource sur laquelle la politique agit. Le champ *`context`* représente un contexte supplémentaire sur le type de politique, qui explique pourquoi l'accès est refusé.

Lorsqu'une politique refuse explicitement l'accès parce qu'elle contient une instruction `Deny`, le message d'erreur de refus d'accès inclut l'expression `with an explicit deny in a` *`type`* `policy`. Lorsque l'accès est implicitement refusé, le message d'erreur de refus d'accès inclut l'expression `because no` *`type`* `policy allows the` *`action`* `action`.

Important

- Les messages de refus d'accès amélioré ne sont renvoyés que pour les demandes portant sur le même compte ou pour les demandes émanant de la même organisation dans. AWS Organizations Les demandes entre comptes extérieurs à la même organisation renvoient un `Access Denied` message générique.

  Pour plus d'informations sur la logique d'évaluation des politiques qui détermine si une demande d'accès intercompte est autorisée ou refusée, consultez Logique d'évaluation des politiques entre comptes dans le Guide de l'utilisateur IAM. Pour voir une procédure détaillée qui décrit comment accorder l'accès intercompte, consultez the section called "Octroi d'autorisations entre comptes".
- Pour les demandes au sein de la même organisation en AWS Organizations :
  - Les messages de refus d'accès amélioré ne sont pas renvoyés si un refus survient en raison d'une politique de point de terminaison de cloud privé virtuel (VPC).
  - Des messages de refus d'accès améliorés sont fournis chaque fois que le propriétaire du compartiment et le compte de l'appelant appartiennent à la même organisation dans AWS Organizations. Bien que les compartiments configurés avec les paramètres

S3 Object Ownership Bucket préférés ou Object Writer puissent contenir des objets appartenant à différents comptes, la propriété des objets n'a aucune incidence sur les messages de refus d'accès améliorés. Des messages de refus d'accès amélioré sont renvoyés pour toutes les demandes d'objet tant que le propriétaire du compartiment et l'appelant appartiennent à la même organisation, quel que soit le propriétaire de l'objet en question. Pour plus d'informations sur les paramètres et les configurations de propriété des objets, consultezthe section called “Contrôle de la propriété des objets”.

- Les messages d’erreur de refus d’accès améliorés ne sont pas renvoyés pour les demandes adressées aux compartiments de répertoires. Les demandes de compartiment de répertoires renvoient un message `Access Denied` générique.
- Si plusieurs politiques de même type refusent une demande d’autorisation, le message d’erreur de refus d’accès ne spécifie pas le nombre de politiques.
- Si une demande d’autorisation est refusée en raison de plusieurs types de politiques, le message d’erreur n’inclut qu’un seul de ces types de politiques.
- Si une demande d’accès est refusée pour plusieurs raisons, le message d’erreur ne comprend qu’une seule des raisons du refus.

Les exemples suivants montrent le format de différents types de messages d’erreur de refus d’accès et indiquent comment résoudre les erreurs liées à chaque type de message.

Accès refusé en raison d’une politique de contrôle des ressources : refus explicite

1. Recherchez une `Deny` déclaration pour l'action dans vos politiques de contrôle des ressources (RCPs). Pour l’exemple suivant, l’action est `s3:GetObject`.
2. Mettez à jour votre politique de contrôle des ressources en supprimant l’instruction `Deny`. Pour plus d’informations, consultez Mise à jour d’une politique de contrôle des ressources dans le Guide de l’utilisateur AWS Organizations .

```
An error occurred (AccessDenied) when calling the GetObject operation:
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
with an explicit deny in a resource control policy
```

Accès refusé en raison d'une politique de contrôle des services - refus implicite

1. Vérifiez qu'il n'y a pas de `Allow` déclaration manquante concernant l'action dans vos politiques de contrôle des services (SCPs). Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour votre SCP en ajoutant l'instruction `Allow`. Pour plus d'information, consultez Mise à jour d'une stratégie de contrôle de service (SCP) dans le Guide de l'utilisateur AWS Organizations .

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject because no service control policy allows the s3:GetObject action
```

Accès refusé en raison d'une politique de contrôle des services - refus explicite

1. Recherchez une `Deny` déclaration pour l'action dans vos politiques de contrôle des services (SCPs). Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour votre politique de contrôle des services en modifiant l'instruction `Deny` pour accorder à l'utilisateur l'accès nécessaire. Pour obtenir un exemple de la marche à suivre, consultez Empêcher les utilisateurs et les rôles IAM d'apporter des modifications spécifiées, à l'exception d'un rôle administrateur spécifié dans le Guide de l'utilisateur AWS Organizations . Pour plus d'informations sur la mise à jour de votre politique de contrôle des services, consultez Mise à jour d'une politique de contrôle des services (SCP) dans le Guide de l'utilisateur AWS Organizations .

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a service control policy
```

Accès refusé en raison d'une politique de point de terminaison d'un VPC : refus implicite

1. Vérifiez l'absence d'une instruction `Allow` pour l'action dans les politiques de votre point de terminaison de cloud privé virtuel (VPC). Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour la politique de point de terminaison d'un VPC en ajoutant l'instruction `Allow`. Pour plus d'informations, consultez la rubrique Mise à jour d'une politique de point de terminaison d'un VPC dans le Guide AWS PrivateLink .

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no VPC endpoint policy allows the s3:GetObject action
```

Accès refusé en raison d'une politique de point de terminaison d'un VPC : refus explicite

1. Vérifiez la présence d'une instruction `Deny` explicite pour l'action dans les politiques de votre point de terminaison de cloud privé virtuel (VPC). Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour la politique de point de terminaison de votre VPC en modifiant l'instruction `Deny` pour accorder à l'utilisateur l'accès nécessaire. Par exemple, vous pouvez mettre à jour l'instruction `Deny` pour utiliser la clé de condition `aws:PrincipalAccount` avec l'opérateur de condition `StringNotEquals` afin d'autoriser l'accès spécifique du principal, comme indiqué dans the section called "Exemple 7 : Exclure des principaux d'instructions Deny". Pour plus d'informations sur la mise à jour de la politique de point de terminaison de votre VPC, consultez Mise à jour d'une politique de point de terminaison d'un VPC dans le Guide AWS PrivateLink .

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a VPC endpoint policy
```

Accès refusé en raison d'une limite des autorisations : refus implicite

1. Vérifiez l'absence d'une instruction `Allow` pour l'action dans votre limite des autorisations. Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour votre limite des autorisations en ajoutant l'instruction `Allow` à votre politique IAM. Pour plus d'informations, consultez Limites d'autorisations pour les entités IAM et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
because no permissions boundary allows the s3:GetObject action
```

Accès refusé en raison d'une limite des autorisations : refus explicite

1. Vérifiez la présence d'une instruction `Deny` explicite pour l'action dans votre limite des autorisations. Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour votre limite d'autorisations en modifiant l'instruction `Deny` dans votre politique IAM pour accorder à l'utilisateur l'accès nécessaire. Par exemple, vous pouvez mettre à jour l'instruction `Deny` pour utiliser la clé de condition `aws:PrincipalAccount` avec l'opérateur de condition `StringNotEquals` afin d'autoriser l'accès spécifique du principal, comme indiqué

dans aws:PrincipalAccount dans le Guide de l'utilisateur IAM. Pour plus d'informations, consultez Limites d'autorisations pour les entités IAM et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

```
User: arn:aws:iam::777788889999:user/MaryMajor is not authorized to perform:
s3:GetObject with an explicit deny in a permissions boundary
```

Accès refusé en raison de politiques de session : refus implicite

1. Vérifiez l'absence d'une instruction `Allow` pour l'action dans vos politiques de session. Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour votre politique de session en ajoutant l'instruction `Allow`. Pour plus d'informations, consultez Politiques de session et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no session policy allows the s3:GetObject action
```

Accès refusé en raison de politiques de session : refus explicite

1. Vérifiez la présence d'une instruction `Deny` explicite pour l'action dans vos politiques de session. Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour la politique de session en modifiant l'instruction `Deny` pour accorder à l'utilisateur l'accès nécessaire. Par exemple, vous pouvez mettre à jour l'instruction `Deny` pour utiliser la clé de condition `aws:PrincipalAccount` avec l'opérateur de condition `StringNotEquals` afin d'autoriser l'accès spécifique du principal, comme indiqué dans the section called "Exemple 7 : Exclure des principaux d'instructions Deny". Pour plus d'informations sur la mise à jour de votre politique de session, consultez Politiques de session et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a session policy
```

Accès refusé en raison de politiques basées sur les ressources : refus implicite

> **Note**
>
> Les politiques basées sur les ressources incluent notamment les politiques de compartiment et les stratégies de point d'accès.

1. Vérifiez l'absence d'une instruction `Allow` pour l'action dans votre politique basée sur les ressources. Vérifiez également si le paramètre de blocage de l'accès public S3 `IgnorePublicAcls` est appliqué au niveau du compartiment, du point d'accès ou du compte. Pour l'exemple suivant, l'action est `s3:GetObject`.
2. Mettez à jour votre politique en ajoutant l'instruction `Allow`. Pour plus d'informations, consultez Politiques basées sur les ressources et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

   Vous devrez peut-être aussi ajuster le paramètre de blocage de l'accès public `IgnorePublicAcls` pour le compartiment, le point d'accès ou le compte. Pour plus d'informations, consultez the section called "Accès refusé en raison de paramètres de blocage de l'accès public" et the section called "Configuration des paramètres de compartiment et de point d'accès".

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no resource-based policy allows the s3:GetObject action
```

Accès refusé en raison de politiques basées sur les ressources : refus explicite

> **Note**
>
> Les politiques basées sur les ressources incluent notamment les politiques de compartiment et les stratégies de point d'accès.

1. Vérifiez la présence d'une instruction `Deny` explicite pour l'action dans votre politique basée sur les ressources. Vérifiez également si le paramètre de blocage de l'accès public S3 `RestrictPublicBuckets` est appliqué au niveau du compartiment, du point d'accès ou du compte. Pour l'exemple suivant, l'action est `s3:GetObject`.

2. Mettez à jour la politique en modifiant l'instruction `Deny` pour accorder à l'utilisateur l'accès nécessaire. Par exemple, vous pouvez mettre à jour l'instruction `Deny` pour utiliser la clé de condition `aws:PrincipalAccount` avec l'opérateur de condition `StringNotEquals` afin d'autoriser l'accès spécifique du principal, comme indiqué dans the section called "Exemple 7 : Exclure des principaux d'instructions Deny". Pour plus d'informations sur la mise à jour d'une politique basée sur les ressources, consultez les sections Politiques basées sur les ressources et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

   Vous devrez peut-être aussi ajuster le paramètre de blocage de l'accès public `RestrictPublicBuckets` pour le compartiment, le point d'accès ou le compte. Pour plus d'informations, consultez the section called "Accès refusé en raison de paramètres de blocage de l'accès public" et the section called "Configuration des paramètres de compartiment et de point d'accès".

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

Accès refusé en raison de politiques basées sur l'identité : refus implicite

1. Vérifiez l'absence d'une instruction `Allow` pour l'action dans les politiques basées sur l'identité attachées à l'identité. Pour l'exemple suivant, l'action est `s3:GetObject` attachée à l'utilisateur `MaryMajor`.
2. Mettez à jour votre politique en ajoutant l'instruction `Allow`. Pour plus d'informations, consultez Politiques basées sur l'identité et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject because no identity-based policy allows the s3:GetObject action
```

Accès refusé en raison de politiques basées sur l'identité : refus explicite

1. Vérifiez la présence d'une instruction `Deny` explicite pour l'action dans les politiques basées sur l'identité attachées à l'identité. Pour l'exemple suivant, l'action est `s3:GetObject` attachée à l'utilisateur `MaryMajor`.
2. Mettez à jour la politique en modifiant l'instruction `Deny` pour accorder à l'utilisateur l'accès nécessaire. Par exemple, vous pouvez mettre à jour l'instruction `Deny` pour utiliser la clé de

condition `aws:PrincipalAccount` avec l'opérateur de condition `StringNotEquals` afin d'autoriser l'accès spécifique du principal, comme indiqué dans aws:PrincipalAccount dans le Guide de l'utilisateur IAM. Pour plus d'informations, consultez Politiques basées sur l'identité et Modification des politiques IAM dans le Guide de l'utilisateur IAM.

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in an identity-based policy
```

Accès refusé en raison de paramètres de blocage de l'accès public

La fonction du blocage de l'accès public Amazon S3 fournit des paramètres pour les points d'accès, les compartiments et les comptes afin de vous aider à gérer l'accès public aux ressources Amazon S3. Pour plus d'informations sur comment Amazon S3 définit le terme « public », consultez La signification du mot « public ».

Par défaut, les nouveaux compartiments, points d'accès et objets n'autorisent pas l'accès public. Toutefois, les utilisateurs peuvent modifier les politiques relatives aux compartiments, les politiques relatives aux points d'accès, les politiques utilisateur IAM, les autorisations relatives aux objets ou les listes de contrôle d'accès (ACLs) pour autoriser l'accès public. Les paramètres d'accès public de S3 Block remplacent ces politiques, autorisations et ACLs. Depuis avril 2023, tous les paramètres de blocage de l'accès public sont activés par défaut pour les nouveaux compartiments.

Quand Amazon S3 reçoit une demande d'accès à un compartiment ou à un objet, il détermine si le paramètre de blocage de l'accès public est défini pour le compartiment ou le compte du propriétaire de compartiment. Si la demande a été effectuée via un point d'accès, Amazon S3 vérifie également les paramètres de blocage de l'accès public pour le point d'accès. S'il existe un paramètre de blocage de l'accès public interdisant l'accès demandé, Amazon S3 rejette la demande.

Le blocage de l'accès public Amazon S3 fournit quatre paramètres. Ces paramètres sont indépendants et peuvent être fournis sous n'importe quelle combinaison. Chaque paramètre peut être appliqué à un point d'accès, à un bucket ou à un AWS compte complet. Si les paramètres de blocage de l'accès public pour le point d'accès, le compartiment ou le compte diffèrent, Amazon S3 applique la combinaison la plus restrictive des paramètres du point d'accès, du compartiment et du compte.

Quand Amazon S3 évalue si une opération est interdite par un paramètre de blocage de l'accès public, il rejette toute demande qui irait à l'encontre d'un paramètre de point d'accès, de compartiment ou de compte.

Les quatre paramètres fournis par le blocage de l'accès public Amazon S3 sont les suivants :

- `BlockPublicAcls` : ce paramètre s'applique aux demandes `PutBucketAcl`, `PutObjectAcl`, `PutObject`, `CreateBucket`, `CopyObject` et `POST Object`. Le paramètre `BlockPublicAcls` entraîne le comportement suivant :
  - Les appels `PutBucketAcl` et `PutObjectAcl` échouent si la liste de contrôle d'accès (ACL) spécifiée est publique.
  - Les appels `PutObject` échouent si la demande inclut une ACL publique.
  - Si ce paramètre est appliqué à un compte, les appels `CreateBucket` échouent avec une réponse HTTP `400` (`Bad Request`) si la demande inclut une ACL publique.

  Par exemple, lorsque l'accès à une demande `CopyObject` est refusé en raison du paramètre `BlockPublicAcls`, vous recevez le message suivant :

  ```
  An error occurred (AccessDenied) when calling the CopyObject operation:
  User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
  perform: s3:CopyObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name"
  because public access control lists (ACLs) are blocked by the BlockPublicAcls block
  public access setting.
  ```

- `IgnorePublicAcls`— Ce `IgnorePublicAcls` paramètre oblige Amazon S3 à ignorer tout ACLs le public d'un bucket et tous les objets qu'il contient. Si l'autorisation de votre demande est accordée uniquement par une liste ACL publique, alors le paramètre `IgnorePublicAcls` rejette la demande.

  Tout refus résultant du paramètre `IgnorePublicAcls` est implicite. Par exemple, si une liste `IgnorePublicAcls` refuse une demande `GetObject` en raison d'une ACL publique, vous recevez le message suivant :

  ```
  User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
  s3:GetObject because no resource-based policy allows the s3:GetObject action
  ```

- `BlockPublicPolicy` : ce paramètre s'applique aux demandes `PutBucketPolicy` et `PutAccessPointPolicy`.

  En définissant `BlockPublicPolicy` pour un compartiment, Amazon S3 rejette les appels à `PutBucketPolicy` si la politique de compartiment spécifiée autorise l'accès public. Ce paramètre conduit également Amazon S3 à rejeter les appels à `PutAccessPointPolicy` pour tous les points d'accès du même compte du compartiment si la politique spécifiée autorise l'accès public.

Si vous définissez `BlockPublicPolicy` pour un point d'accès, Amazon S3 rejette les appels `PutAccessPointPolicy` et `PutBucketPolicy` qui sont effectués via le point d'accès si la stratégie ou la politique spécifiée (pour le point d'accès ou le compartiment sous-jacent) autorise l'accès public.

Par exemple, lorsque l'accès est refusé dans une demande `PutBucketPolicy` en raison du paramètre `BlockPublicPolicy`, vous recevez le message suivant :

```
An error occurred (AccessDenied) when calling the PutBucketPolicy operation:
User: arn:aws:sts::123456789012:user/MaryMajor is not authorized to
perform: s3:PutBucketPolicy on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-
name"
because public policies are blocked by the BlockPublicPolicy block public
access setting.
```

- `RestrictPublicBuckets`— Le `RestrictPublicBuckets` paramètre restreint l'accès à un point d'accès ou à un bucket soumis à une politique publique uniquement aux Service AWS principaux et aux utilisateurs autorisés du compte du propriétaire du bucket et du compte du propriétaire du point d'accès. Ce paramètre bloque tous les accès entre comptes au point d'accès ou au compartiment (sauf pour Service AWS les principaux), tout en permettant aux utilisateurs du compte de gérer le point d'accès ou le compartiment. Ce paramètre rejette également tous les appels anonymes (ou non signés).

  Tout refus résultant du paramètre `RestrictPublicBuckets` est explicite. Par exemple, si une liste `RestrictPublicBuckets` refuse une demande `GetObject` en raison d'une politique de compartiment public ou de point d'accès, vous recevez le message suivant :

```
User: arn:aws:iam::123456789012:user/MaryMajor is not authorized to perform:
s3:GetObject on resource: "arn:aws:s3:::amzn-s3-demo-bucket1/object-name" with
an explicit deny in a resource-based policy
```

Pour plus d'informations sur ces paramètres, consultez la page the section called "Paramètres de la fonctionnalité de blocage de l'accès public". Pour vérifier et mettre à jour ces paramètres, consultez the section called "Configuration du blocage d'accès public".

Politiques de compartiment et politiques IAM

Opérations au niveau des compartiments

Si aucune politique de compartiment n'est en place, le compartiment autorise implicitement les demandes provenant de n'importe quelle identité AWS Identity and Access Management (IAM) du compte du propriétaire du compartiment. Le compartiment refuse également implicitement les demandes émanant de toute autre identité IAM provenant d'autres comptes, ainsi que les demandes anonymes (non signées). Toutefois, si aucune politique utilisateur IAM n'est en place, le demandeur (sauf s'il s'agit de l'utilisateur Compte AWS root) se voit implicitement refuser le droit de faire des demandes. Pour plus d'informations sur cette logique d'évaluation, consultez Identification d'une demande autorisée ou refusée dans un compte dans le Guide de l'utilisateur d'IAM.

Opérations au niveau de l'objet

Si l'objet appartient au compte propriétaire du compartiment, la politique de compartiment et la politique de l'utilisateur IAM fonctionneront de la même manière pour les opérations au niveau de l'objet que pour les opérations au niveau du compartiment. Par exemple, si aucune politique de compartiment n'est en place, le compartiment autorise implicitement les demandes d'objet provenant de n'importe quelle identité IAM du compte du propriétaire du compartiment. Le compartiment refuse également implicitement les demandes d'objet émanant de toute autre identité IAM provenant d'autres comptes, ainsi que les demandes anonymes (non signées). Toutefois, si aucune politique utilisateur IAM n'est en place, le demandeur (sauf s'il s'agit de l'utilisateur Compte AWS root) se voit implicitement refuser le droit de faire des demandes d'objet.

Si l'objet appartient à un compte externe, l'accès à l'objet ne peut être accordé que par le biais de listes de contrôle d'accès aux objets (ACLs). La politique relative aux compartiments et la politique d'utilisateur IAM peuvent toujours être utilisées pour refuser les demandes d'objets.

Par conséquent, pour vous assurer que votre politique de compartiment ou votre politique d'utilisateur IAM n'est pas à l'origine d'une erreur d'accès refusé (403 Forbidden), assurez-vous que les conditions suivantes sont remplies :

- Pour l'accès au même compte, aucune déclaration `Deny` explicite ne doit être formulée à l'encontre du demandeur auquel vous essayez d'accorder des autorisations, que ce soit dans la politique de compartiment ou dans la politique d'utilisateur IAM. Si vous souhaitez accorder des autorisations en utilisant uniquement la politique de compartiment et la politique d'utilisateur IAM, l'une de ces politiques doit contenir au moins une déclaration `Allow` explicite.

- Pour l'accès intercompte, aucune instruction `Deny` explicite ne doit être formulée à l'encontre du demandeur auquel vous essayez d'accorder des autorisations, que ce soit dans la politique de compartiment ou dans la politique d'utilisateur IAM. Si vous souhaitez accorder des autorisations intercomptes en utilisant uniquement la politique de compartiment et la politique d'utilisateur IAM, assurez-vous que la politique de compartiment et la politique d'utilisateur IAM du demandeur incluent une instruction `Allow` explicite.

> **Note**
>
> Les déclarations `Allow` d'une politique de compartiment s'appliquent uniquement aux objets appartenant au même compte propriétaire du compartiment. Toutefois, les déclarations `Deny` figurant dans une politique de compartiment s'appliquent à tous les objets, quel que soit leur propriétaire.

Pour consulter ou modifier votre politique de compartiment

> **Note**
>
> Pour afficher ou modifier une politique de compartiment, vous devez disposer de l'autorisation `s3:GetBucketPolicy`.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment pour lequel vous souhaitez afficher ou modifier une politique de compartiment.
4. Sélectionnez l'onglet Autorisations.
5. Sous Politique de compartiment, choisissez Modifier. La page Edit bucket policy (Modifier la politique de compartiment) s'affiche.

Pour revoir ou modifier votre politique de compartiment à l'aide de la AWS Command Line Interface (AWS CLI), utilisez la get-bucket-policycommande.

> **Note**
>
> Si l'accès à un compartiment est bloqué en raison d'une politique de compartiment incorrecte, connectez-vous au en AWS Management Console utilisant vos informations d'identification d'utilisateur Compte AWS root. Pour accéder de nouveau à votre bucket, assurez-vous de supprimer la politique de bucket incorrecte en utilisant vos informations d'identification d'utilisateur Compte AWS root.

Conseils pour vérifier les autorisations

Pour vérifier si le demandeur dispose des autorisations nécessaires pour effectuer une opération Amazon S3, essayez ce qui suit :

- Identifiez le demandeur. S'il s'agit d'une demande non signée, il s'agit d'une demande anonyme sans politique d'utilisateur IAM. S'il s'agit d'une demande utilisant une URL présignée, la politique d'utilisateur sera la même que celle applicable à l'utilisateur ou au rôle IAM qui a signé la demande.
- Vérifiez que vous utilisez le bon rôle ou utilisateur IAM. Vous pouvez vérifier votre utilisateur ou rôle IAM en vérifiant le coin supérieur droit de la AWS Management Console ou à l'aide de la commande aws sts get-caller-identity.
- Vérifiez les politiques IAM attachées à l'utilisateur ou au rôle IAM. Vous pouvez choisir l'une des méthodes suivantes :
  - Testez des politiques IAM avec le simulateur de politiques IAM.
  - Passez en revue les différents types de politiques IAM.
- Si nécessaire, modifiez votre politique d'utilisateur IAM.
- Consultez les exemples suivants de politiques qui refusent ou autorisent explicitement l'accès :
  - Autoriser explicitement la politique de l'utilisateur IAM : IAM : autorise et refuse l'accès à plusieurs services par programmation et dans la console
  - Politique d'autorisation explicite en matière de compartiment : octroi d'autorisations à plusieurs comptes pour télécharger des objets ou définir un objet ACLs pour un accès public
  - Politique de refus explicite des utilisateurs IAM AWS: refuse l'accès en AWS fonction de la demande Région AWS
  - Refuser explicitement la politique de compartiment : exiger le SSE-KMS pour tous les objets enregistrés dans un compartiment

Paramètres des listes de contrôle d'accès d'Amazon S3

Lorsque vous vérifiez vos paramètres ACL, vérifiez d'abord votre paramètre de propriété des objets pour vérifier s'ils ACLs sont activés sur le bucket. Sachez que les autorisations ACL ne peuvent être utilisées que pour accorder des autorisations et ne peuvent pas être utilisées pour rejeter des demandes. ACLs ne peut pas non plus être utilisé pour accorder l'accès à des demandeurs rejetés par des refus explicites dans les politiques de compartiment ou les politiques utilisateur IAM.

Le paramètre Object Ownership est défini sur Bucket owner (appliqué).

Si le paramètre imposé par le propriétaire du compartiment est activé, il est peu probable que les paramètres ACL provoquent une erreur d'accès refusé (403 Interdit) car ce paramètre désactive tout ce ACLs qui s'applique au compartiment et aux objets. Le paramètre appliqué par le propriétaire du compartiment est le paramètre par défaut (et recommandé) pour les compartiments Amazon S3.

Le paramètre Propriété de l'objet est défini sur « Propriétaire du compartiment préféré » ou « Auteur de l'objet ».

Les autorisations ACL sont toujours valides avec le paramètre préféré du propriétaire du bucket ou le paramètre Object Writer. Il en existe deux types ACLs : un ACLs godet et un objet ACLs. Pour connaître les différences entre ces deux types de ACLs, voir Cartographie des autorisations ACL et des autorisations de politique d'accès.

En fonction de l'action de la demande rejetée, vérifiez les autorisations des listes ACL pour votre compartiment ou l'objet :

- Si Amazon S3 a rejeté `LIST`, un objet `PUT`, `GetBucketAcl` ou une demande `PutBucketAcl`, passez en revue les autorisations des listes ACL pour votre compartiment.

  > **Note**
  >
  > Vous ne pouvez pas accorder d'autorisations d'objets `GET` avec les paramètres des listes ACL du compartiment.

- Si Amazon S3 a rejeté une demande `GET` concernant un objet S3 ou une demande PutObjectAcl, passez en revue les autorisations des listes ACL pour cet objet.

> **Important**
>
> Si le compte qui détient l'objet est différent du compte qui détient le compartiment, l'accès à l'objet n'est pas contrôlé par la politique de compartiment.

Résolution d'une erreur d'accès refusé (403 Forbidden) liée à une demande d'objet **GET** lors de la propriété d'un objet intercompte

Passez en revue les paramètres de propriété de l'objet du compartiment pour déterminer le propriétaire de l'objet. Si vous avez accès à l'objet ACLs, vous pouvez également consulter le compte du propriétaire de l'objet. (Pour consulter le compte du propriétaire de l'objet, consultez le paramètre de la liste ACL de l'objet dans la console Amazon S3.) Vous pouvez également faire une demande `GetObjectAcl` d'identification canonique du propriétaire de l'objet afin de vérifier le compte du propriétaire de l'objet. Par défaut, ACLs accordez des autorisations explicites pour les `GET` demandes adressées au compte du propriétaire de l'objet.

Après avoir confirmé que le propriétaire de l'objet est différent du propriétaire du compartiment, en fonction de votre cas d'utilisation et de votre niveau d'accès, choisissez l'une des méthodes suivantes pour résoudre l'erreur d'accès refusé (403 Forbidden) :

- Désactiver ACLs (recommandé) : cette méthode s'applique à tous les objets et peut être exécutée par le propriétaire du compartiment. Cette méthode offre automatiquement au propriétaire du compartiment la propriété de chaque objet du compartiment et leur contrôle total. Avant d'implémenter cette méthode, vérifiez les conditions préalables à la désactivation ACLs. Pour plus d'informations sur la façon de configurer votre bucket en mode imposé par le propriétaire du bucket (recommandé), consultez la section Définition de la propriété des objets sur un bucket existant.

  > **Important**
  >
  > Pour éviter une erreur d'accès refusé (403 Interdit), veillez à migrer les autorisations ACL vers une politique de compartiment avant de les désactiver ACLs. Pour plus d'informations, consultez Bucket policy examples for migrating from ACL permissions (Exemples de politiques de compartiment pour la migration à partir d'autorisations de listes ACL).

- Remplacer le propriétaire de l'objet par le propriétaire du compartiment : cette méthode peut être appliquée à des objets individuels, mais seul le propriétaire de l'objet (ou un utilisateur disposant des autorisations appropriées) peut modifier la propriété d'un objet. Des frais PUT supplémentaires

peuvent s'appliquer. (Pour plus d'informations, consultez Tarification Amazon S3.) Cette méthode confère au propriétaire du compartiment la pleine propriété de l'objet, ce qui lui permet de contrôler l'accès à l'objet par le biais d'une politique de compartiment.

Pour modifier la propriété de l'objet, effectuez l'une des opérations suivantes :

- Vous (le propriétaire du compartiment) pouvez recopier l'objet dans le compartiment.
- Vous pouvez modifier le paramètre de propriété de l'objet du compartiment sur le paramètre préféré du propriétaire du compartiment. Si la gestion des versions est désactivée, les objets du compartiment sont remplacés. Si la gestion des versions est activée, des versions dupliquées du même objet apparaîtront dans le compartiment, et le propriétaire du compartiment peut définir une règle de cycle de vie d'expiration. Pour plus d'informations sur la modification des paramètres de propriété des objets, consultez Définition de la propriété d'un objet sur un compartiment existant.

  > **Note**
  >
  > Lorsque vous mettez à jour votre paramètre de propriété de l'objet sur la préférence du propriétaire du compartiment, le paramètre est appliqué uniquement aux nouveaux objets chargés dans le compartiment.

- Vous pouvez demander au propriétaire de l'objet de le charger à nouveau à l'aide de la liste ACL de l'objet prédéfini `bucket-owner-full-control`.

> **Note**
>
> Pour les chargements intercomptes, vous pouvez également exiger la liste ACL de l'objet prédéfini `bucket-owner-full-control` dans votre politique de compartiment. Pour un exemple de politique de compartiment, consultez Octroi d'autorisations intercomptes pour charger des objets tout en garantissant que le propriétaire du compartiment dispose d'un contrôle total.

- Conservez le rédacteur de l'objet en tant que propriétaire de l'objet : cette méthode ne modifie pas le propriétaire de l'objet, mais elle vous permet d'accorder l'accès aux objets individuellement. Pour autoriser l'accès à un objet, vous devez disposer de l'autorisation `PutObjectAcl` pour cet objet. Ensuite, pour corriger l'erreur Accès refusé (403 Interdit), ajoutez le demandeur en tant que bénéficiaire pour accéder à l'objet dans celui de l'objet. ACLs Pour de plus amples informations, veuillez consulter Configuration ACLs.

Paramètres de blocage de l'accès public S3

Si l'échec de la demande implique un accès public ou des politiques publiques, vérifiez alors les paramètres de blocage de l'accès public S3 sur votre compte, votre compartiment ou votre point d'accès. Pour plus d'informations sur la résolution des erreurs de refus d'accès liées aux paramètres de blocage de l'accès public S3, consultez the section called "Accès refusé en raison de paramètres de blocage de l'accès public".

Paramètres du chiffrement Amazon S3

Amazon S3 prend en charge le chiffrement côté serveur sur votre compartiment. Le chiffrement côté serveur est le chiffrement des données à leur destination par l'application ou le service qui les reçoit. Amazon S3 chiffre vos données au niveau de l'objet lorsqu'il les écrit sur les disques des centres de AWS données et les déchiffre pour vous lorsque vous y accédez.

Par défaut, Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. Amazon S3 vous permet également de spécifier la méthode de chiffrement côté serveur lors du chargement d'objets.

Pour vérifier le statut et les paramètres de chiffrement côté serveur de votre compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le compartiment pour lequel vous souhaitez vérifier les paramètres de chiffrement.
4. Choisissez l'onglet Propriétés.
5. Faites défiler l'écran vers le bas jusqu'à la section Chiffrement par défaut, puis examinez les paramètres de Type de chiffrement.

Pour vérifier vos paramètres de chiffrement à l'aide de AWS CLI, utilisez la get-bucket-encryptioncommande.

Pour vérifier le statut du chiffrement d'un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment qui contient l'objet.
4. Dans la liste Objets, choisissez le nom de l'objet pour lequel vous souhaitez ajouter ou modifier le chiffrement.

   La page de détails de l'objet s'affiche.
5. Accédez à la section Paramètres de chiffrement côté serveur pour afficher les paramètres de chiffrement côté serveur de l'objet.

Pour vérifier l'état du chiffrement de votre objet à l'aide de AWS CLI, utilisez la head-objectcommande.

Exigences en matière de chiffrement et d'autorisations

Amazon S3 prend en charge trois types de chiffrement côté serveur :

- Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
- Chiffrement côté serveur avec clés AWS Key Management Service (AWS KMS) (SSE-KMS)
- Chiffrement côté serveur avec clés fournies par le client (SSE-C)

En fonction de vos paramètres de chiffrement, assurez-vous que les exigences d'autorisation suivantes sont remplies :

- SSE-S3 : aucune autorisation supplémentaire n'est requise.
- SSE-KMS (avec une clé gérée par le client) : pour télécharger des objets, l'autorisation `kms:GenerateDataKey` est requise sur la AWS KMS key . Pour télécharger des objets et effectuer des chargements partitionnés d'objets, l'autorisation `kms:Decrypt` est requise sur la clé KMS.
- SSE-KMS (avec un Clé gérée par AWS) — Le demandeur doit être associé au même compte que celui qui possède la `aws/s3` clé KMS. Le demandeur doit également disposer des autorisations Amazon S3 appropriées pour accéder à l'objet.
- SSE-C (avec une clé fournie par le client) : aucune autorisation supplémentaire n'est requise. Vous pouvez configurer la politique de compartiment pour exiger et restreindre le chiffrement côté serveur avec les clés de chiffrement fournies par le client pour les objets de votre compartiment.

Si l'objet est chiffré à l'aide d'une clé gérée par le client, assurez-vous que la stratégie de clé KMS vous permet d'effectuer les actions `kms:GenerateDataKey` ou `kms:Decrypt`. Pour obtenir des instructions sur la vérification de votre stratégie de clé KMS, consultez Viewing a key policy (Affichage d'une politique relative aux clés) dans le Guide du développeur AWS Key Management Service .

Paramètres de verrouillage des objets S3

Si le verrouillage d'objet S3 est activé sur votre compartiment et que l'objet est protégé par une période de rétention ou une conservation légale, Amazon S3 renvoie une erreur d'accès refusé (403 Forbidden) lorsque vous essayez de supprimer l'objet.

Pour vérifier si le verrouillage des objets est activé sur le compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment que vous souhaitez vérifier.
4. Choisissez l'onglet Propriétés.
5. Faites défiler jusqu'à la section Verrouillage des objets. Vérifiez si le paramètre Verrouillage des objets est Activé ou Désactivé.

Pour déterminer si l'objet est protégé par une période de rétention ou une conservation légale, consultez les informations de verrouillage de votre objet.

Si l'objet est protégé par une période de rétention ou une conservation légale, vérifiez les points suivants :

- Si la version de l'objet est protégée par le mode de conservation de la conformité, il n'est pas possible de la supprimer définitivement. Une `DELETE` demande permanente émanant d'un demandeur, y compris de l'utilisateur Compte AWS root, entraînera une erreur d'accès refusé (403 Interdit). Sachez également que lorsque vous soumettez une demande `DELETE` pour un objet protégé par le mode de conservation de la conformité, Amazon S3 crée un marqueur de suppression pour cet objet.
- Si la version de l'objet est protégée par le mode de conservation de la gouvernance et que vous en avez l'autorisation `s3:BypassGovernanceRetention`, vous pouvez contourner la protection et supprimer définitivement la version. Pour plus d'informations, consultez Ignorer le mode de gouvernance.

- Si la version de l'objet est protégée par une conservation légale, une demande `DELETE` permanente peut entraîner une erreur d'accès refusé (403 Forbidden). Pour supprimer définitivement la version de l'objet, vous devez supprimer la conservation légale sur la version de l'objet. Pour supprimer une conservation légale, vous devez avoir l'autorisation `s3:PutObjectLegalHold`. Pour plus d'informations sur la suppression d'une conservation légale, consultez Configuration du verrouillage d'objet S3.

Politiques de point de terminaison d'un VPC

Si vous accédez à Amazon S3 en utilisant le point de terminaison d'un cloud privé virtuel (VPC), assurez-vous que la politique de point de terminaison du VPC ne vous empêche pas d'accéder à vos ressources Amazon S3. Par défaut, la politique de point de terminaison d'un VPC autorise toutes les demandes adressées à Amazon S3. Vous pouvez également configurer la politique de point de terminaison d'un VPC pour restreindre certaines demandes. Pour plus d'informations sur la vérification de votre politique de point de terminaison d'un VPC, consultez les ressources suivantes :

- the section called "Accès refusé en raison d'une politique de point de terminaison d'un VPC : refus implicite"
- the section called "Accès refusé en raison d'une politique de point de terminaison d'un VPC : refus explicite"
- Contrôle de l'accès aux points de terminaison d'un VPC à l'aide des politiques de point de terminaison d'un VPC dans le Guide AWS PrivateLink .

AWS Organizations politiques

Si vous Compte AWS appartenez à une organisation, AWS Organizations les politiques peuvent vous empêcher d'accéder aux ressources Amazon S3. Par défaut, AWS Organizations les politiques ne bloquent aucune demande adressée à Amazon S3. Assurez-vous toutefois que vos AWS Organizations politiques n'ont pas été configurées pour bloquer l'accès aux compartiments S3. Pour savoir comment vérifier vos AWS Organizations politiques, consultez les ressources suivantes :

- the section called "Accès refusé en raison d'une politique de contrôle des services - refus implicite"
- the section called "Accès refusé en raison d'une politique de contrôle des services - refus explicite"
- the section called "Accès refusé en raison d'une politique de contrôle des ressources : refus explicite"
- Liste de toutes les politiques dans le Guide de l'utilisateur AWS Organizations

En outre, si vous avez configuré votre politique de compartiment de manière incorrecte pour qu'un compte membre refuse à tous les utilisateurs l'accès à votre compartiment S3, vous pouvez déverrouiller le compartiment en lançant une session privilégiée pour ce compte membre dans IAM. Après avoir lancé une session privilégiée, vous pouvez supprimer la politique de compartiment mal configurée pour retrouver l'accès au compartiment. Pour plus d'informations, voir Exécuter une tâche privilégiée sur un compte AWS Organizations membre dans le Guide de AWS Identity and Access Management l'utilisateur.

CloudFront accès à la distribution

Si vous recevez un message d'erreur Accès refusé (403 Interdit) lorsque vous essayez d'accéder à votre site Web statique S3 CloudFront, vérifiez les problèmes courants suivants :

- Avez-vous le bon format de nom de domaine d'origine ?
  - Assurez-vous d'utiliser le format de point de terminaison du site Web S3 (bucket-name.s3-website-region.amazonaws.com) plutôt que le point de terminaison de l'API REST
  - Vérifiez que l'hébergement statique de sites Web est activé sur votre compartiment
- Votre politique relative aux compartiments autorise-t-elle CloudFront l'accès ?
  - Assurez-vous que votre politique de compartiment inclut des autorisations pour l'identité d'accès à l'origine (OAI) ou le contrôle d'accès à l'origine (OAC) de votre CloudFront distribution
  - Vérifiez que la politique inclut les GetObject autorisations s3 : requises

Pour des étapes de résolution des problèmes et des configurations supplémentaires, y compris les configurations des pages d'erreur et les paramètres du protocole, consultez Pourquoi le message d'erreur « 403 accès refusé » s'affiche lorsque j'utilise un point de terminaison d'un site Web Amazon S3 comme origine de ma CloudFront distribution ? dans le AWS re:Post Knowledge Center.

> **Note**
>
> Cette erreur est différente des erreurs 403 que vous pourriez recevoir en accédant directement à S3. Pour les problèmes CloudFront spécifiques, assurez-vous de vérifier à la fois vos paramètres de CloudFront distribution et vos configurations S3.

Paramètres du point d'accès

Si vous recevez un message d'erreur d'accès refusé (403 Forbidden) lorsque vous effectuez des demandes via les points d'accès Amazon S3, vous devrez peut-être vérifier les points suivants :

- Les configurations de vos points d'accès
- La politique d'utilisateur IAM utilisée pour vos points d'accès
- La politique de compartiment utilisée pour gérer ou configurer vos points d'accès intercompte

Configurations et politiques des points d'accès

- Lorsque vous créez un point d'accès, vous pouvez choisir de désigner Internet ou VPC comme l'origine du réseau. Si l'origine du réseau est définie sur VPC uniquement, Amazon S3 rejettera toutes les demandes adressées au point d'accès qui ne proviennent pas du VPC spécifié. Pour vérifier l'origine du réseau de votre point d'accès, consultez Création de points d'accès restreints à un virtual private cloud.
- Avec les points d'accès, vous pouvez également configurer des paramètres personnalisés de blocage de l'accès public, qui fonctionnent de la même manière que les paramètres de blocage de l'accès public au niveau du compartiment ou du compte. Pour vérifier vos paramètres personnalisés de blocage de l'accès public, consultez Gestion de l'accès public aux points d'accès pour les compartiments à usage général.
- Pour envoyer des demandes réussies à Amazon S3 à l'aide de points d'accès, assurez-vous que le demandeur dispose des autorisations IAM nécessaires. Pour de plus amples informations, veuillez consulter Configuration des politiques IAM pour l'utilisation des points d'accès.
- Si la demande concerne des points d'accès intercompte, assurez-vous que le propriétaire du compartiment a mis à jour la politique du compartiment pour autoriser les demandes provenant du point d'accès. Pour de plus amples informations, veuillez consulter Octroi d'autorisations pour les points d'accès intercompte.

Si l'erreur Accès refusé (403 Interdit) persiste après avoir vérifié tous les éléments de cette rubrique, récupérez votre identifiant de demande Amazon S3 et contactez-nous Support pour obtenir des conseils supplémentaires.

Ressources supplémentaires

Pour plus d'informations sur les erreurs d'accès refusé (403 Interdit), vous pouvez consulter les ressources suivantes :

- Comment résoudre les erreurs 403 Access Denied depuis Amazon S3 ? dans le AWS re:Post Knowledge Center.
- Pourquoi le message d'erreur 403 Forbidden s'affiche-t-il lorsque j'essaie d'accéder à un compartiment ou à un objet Amazon S3 ? dans le AWS re:Post Knowledge Center.
- Pourquoi le message d'erreur Accès refusé s'affiche-t-il lorsque j'essaie d'accéder à une ressource Amazon S3 dans le même espace Compte AWS ? dans le AWS re:Post Knowledge Center.
- Pourquoi le message d'erreur Accès refusé s'affiche-t-il lorsque j'essaie d'accéder à un compartiment Amazon S3 avec un accès public en lecture ? dans le AWS re:Post Knowledge Center.
- Pourquoi le message d'erreur « signature non concordance » s'affiche-t-il lorsque j'essaie d'utiliser une URL présignée pour charger un objet sur Amazon S3 ? dans le AWS re:Post Knowledge Center.
- Pourquoi est-ce que je reçois un message d'erreur d'accès refusé pour la ListObjects version V2 lorsque j'exécute la commande de synchronisation sur mon compartiment Amazon S3 ? dans le AWS re:Post Knowledge Center.
- Pourquoi le message d'erreur « 403 accès refusé » s'affiche-t-il lorsque j'utilise un point de terminaison d'un site Web Amazon S3 comme origine de ma CloudFront distribution ? dans le AWS re:Post Knowledge Center.

AWS politiques gérées pour Amazon S3

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 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.

AWS politique gérée : AmazonS3FullAccess

Vous pouvez attacher la politique `AmazonS3FullAccess` à vos identités IAM. Cette politique accorde des autorisations qui permettent un accès complet à Amazon S3.

Pour consulter les autorisations relatives à cette politique, consultez AmazonS3FullAccess dans AWS Management Console.

AWS politique gérée : AmazonS3ReadOnlyAccess

Vous pouvez attacher la politique `AmazonS3ReadOnlyAccess` à vos identités IAM. Cette politique accorde des autorisations qui permettent d'accéder en lecture seule à Amazon S3.

Pour consulter les autorisations relatives à cette politique, consultez AmazonS3ReadOnlyAccess dans AWS Management Console.

Politique gérée par AWS : AmazonS3ObjectLambdaExecutionRolePolicy

Fournit aux AWS Lambda fonctions les autorisations requises pour envoyer des données à S3 Object Lambda lorsque des demandes sont adressées à un point d'accès S3 Object Lambda. Accorde également à Lambda l'autorisation d'écrire dans les journaux Amazon CloudWatch .

Pour consulter les autorisations relatives à cette politique, consultez AmazonS3ObjectLambdaExecutionRolePolicy dans AWS Management Console.

Politique gérée par AWS : S3UnlockBucketPolicy

Si vous avez mal configuré votre politique de compartiment pour qu'un compte membre refuse à tous les utilisateurs l'accès à votre compartiment S3, vous pouvez utiliser cette politique AWS gérée (`S3UnlockBucketPolicy`) pour déverrouiller le compartiment. Pour plus d'informations sur la manière de supprimer une politique de compartiment mal configurée qui empêche tous les principaux d'accéder à un compartiment Amazon S3, consultez la section Exécuter une tâche privilégiée sur un compte AWS Organizations membre dans le Guide de l'AWS Identity and Access Management utilisateur.

Amazon S3 met à jour les politiques AWS gérées

Consultez les informations relatives aux mises à jour des politiques AWS gérées pour Amazon S3 depuis que ce service a commencé à suivre ces modifications.

Modification	Description	Date
Amazon S3 a ajouté `S3UnlockBucketPolicy`	Amazon S3 a ajouté une nouvelle politique AWS gérée appelée `S3UnlockBucketPolicy` à déverrouiller un compartiment et à supprimer une politique de compartiment mal configurée qui empêche tous les principaux d'accéder à un compartiment Amazon S3.	1er novembre 2024
Amazon S3 a ajouté des autorisations Describe à `AmazonS3ReadOnlyAccess`	Amazon S3 a ajouté des autorisations `s3:Describe*` à `AmazonS3ReadOnlyAccess` .	11 août 2023
Amazon S3 a ajouté des autorisations S3 Object Lambda à `AmazonS3FullAccess` et `AmazonS3ReadOnlyAccess` .	Amazon S3 a mis à jour les politiques `AmazonS3FullAccess` et `AmazonS3ReadOnlyAccess` pour inclure les autorisations pour S3 Object Lambda.	27 septembre 2021
Amazon S3 a ajouté `AmazonS3ObjectLambdaExecutionRolePolicy`	Amazon S3 a ajouté une nouvelle politique AWS gérée appelée `AmazonS3ObjectLambdaExecutionRolePolicy` qui fournit aux fonctions Lambda des autorisations leur permettant d'interagir avec S3 Object	18 août 2021

Modification	Description	Date
	Lambda et d'écrire dans des journaux. CloudWatch	
Amazon S3 a commencé à assurer le suivi des modifications	Amazon S3 a commencé à suivre les modifications apportées AWS à ses politiques gérées.	18 août 2021

Gestion de l'accès aux jeux de données avec des points d'accès

Les points d'accès Amazon S3 simplifient l'accès aux données pour tout AWS service ou application client qui stocke des données dans S3. Les points d'accès sont appelés points de terminaison réseau attachés à une source de données telle qu'un bucket ou un volume Amazon FSx pour OpenZFS. Pour plus d'informations sur l'utilisation des compartiments, consultez Présentation des compartiments à usage général. Pour plus d'informations sur l'utilisation d' FSx OpenZFS, consultez la section Qu'est-ce qu'Amazon FSx pour OpenZFS dans le guide de l'utilisateur d'OpenZFS.

Vous pouvez utiliser des points d'accès pour effectuer des opérations sur des objets S3, telles que `GetObject` et`PutObject`. Chaque point d'accès dispose d'autorisations et de contrôles réseau distincts que S3 applique pour toute demande effectuée via ce point d'accès. Chaque point de terminaison applique une politique de point d'accès personnalisée qui vous permet de contrôler l'utilisation par ressource, par utilisateur ou selon d'autres conditions. Si votre point d'accès est attaché à un bucket, la politique de point d'accès fonctionne conjointement avec la politique de bucket sous-jacente. Vous pouvez configurer n'importe quel point d'accès pour accepter uniquement les demandes provenant d'un cloud privé virtuel (VPC) afin de restreindre l'accès aux données Amazon S3 à un réseau privé. Vous pouvez également configurer des paramètres de blocage de l'accès public personnalisés pour chaque point d'accès.

> **Note**
>
> Vous ne pouvez utiliser que des points d'accès pour effectuer des opérations sur des objets. Vous ne pouvez pas utiliser les points d'accès pour effectuer d'autres opérations Amazon S3, telles que la suppression de compartiments ou la création de configurations de réplication S3. Pour obtenir la liste complète des opérations S3 qui prennent en charge les points d'accès, consultez Compatibilité avec les points d'accès.

Les rubriques de cette section expliquent comment utiliser les points d'accès Amazon S3. Pour les rubriques relatives à l'utilisation de points d'accès avec des compartiments de répertoire, voir,Gestion de l'accès aux ensembles de données partagés dans des compartiments d'annuaire dotés de points d'accès.

Rubriques

- Règles, restrictions et limitations de dénomination des points d'accès
- Référencement de points d'accès sous forme d' ARNsalias de point d'accès ou de type hébergé virtuellement URIs
- Compatibilité avec les points d'accès
- Configuration des politiques IAM pour l'utilisation des points d'accès
- Surveillance et journalisation des points d'accès
- Création d'un point d'accès
- Gestion de vos points d'accès Amazon S3 pour les compartiments à usage général
- Utilisation des points d'accès Amazon S3 pour des compartiments à usage général
- Utilisation de balises avec des points d'accès S3 pour des compartiments à usage général

Règles, restrictions et limitations de dénomination des points d'accès

Les points d'accès sont appelés points de terminaison réseau attachés à un compartiment ou à un volume sur un système de FSx fichiers Amazon qui simplifient la gestion des données. Lorsque vous créez un point d'accès, vous choisissez un nom et le Région AWS nom dans lequel le créer. Les rubriques suivantes fournissent des informations sur les règles, restrictions et limitations de dénomination des points d'accès.

Rubriques

- Règles de dénomination pour les points d'accès
- Restrictions et limitations relatives aux points d'accès
- Restrictions et limitations relatives aux points d'accès associés à un volume sur un système de FSx fichiers Amazon

Règles de dénomination pour les points d'accès

Lorsque vous créez un point d'accès, vous choisissez son nom et celui dans lequel le Région AWS créer. Contrairement aux compartiments à usage général, les noms des points d'accès n'ont pas

besoin d'être uniques entre Comptes AWS ou Régions AWS. Cela Compte AWS peut créer des points d'accès portant le même nom dans des langues différentes Régions AWS ou deux points d'accès différents Comptes AWS peuvent utiliser le même nom de point d'accès. Cependant, au sein d'un même Région AWS an, Compte AWS il se peut qu'il n'y ait pas deux points d'accès portant le même nom.

> **Note**
>
> Si vous choisissez de publier le nom de votre point d'accès, évitez d'inclure des informations sensibles dans le nom du point d'accès. Les noms des points d'accès sont publiés dans une base de données accessible au public, appelée système de nom de domaine (DNS).

Les noms des points d'accès doivent être conformes au DNS et répondre aux conditions suivantes :

- Doit être unique au sein d'un seul Compte AWS et Région AWS
- Ils doivent commencer par un chiffre ou une lettre minuscule.
- Ils doivent comporter entre 3 et 50 caractères.
- Ils ne peuvent pas commencer ou se terminer par un trait d'union (-)
- Ne peut pas contenir de traits de soulignement (_), de lettres majuscules, d'espaces ou de points (.)
- Impossible de terminer par le suffixe `-s3alias` ou`-ext-s3alias`. Ces suffixes sont réservés aux noms d'alias des points d'accès. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Restrictions et limitations relatives aux points d'accès

Les points d'accès Amazon S3 comportent les limites et restrictions suivantes :

- Chaque point d'accès est associé à exactement un compartiment ou à un FSx volume OpenZFS. Vous devez le spécifier lorsque vous créez le point d'accès. Après avoir créé un point d'accès, vous ne pouvez pas l'associer à un autre bucket ou à un FSx volume OpenZFS. Vous pouvez toutefois supprimer un point d'accès, puis en créer un autre portant le même nom.
- Après avoir créé un point d'accès, vous ne pouvez pas modifier sa configuration VPC (virtual private cloud).
- Les stratégies de point d'accès sont limitées à une taille de 20 Ko.

- Vous pouvez créer un maximum de 10 000 points d'accès Compte AWS par personne Région AWS. Si vous avez besoin de plus de 10 000 points d'accès pour un seul compte dans une même région, vous pouvez demander une augmentation des quotas de service. Pour plus d'informations sur les quotas de service et la demande d'une augmentation, consultez AWS Service Quotas dans Références générales AWS.
- Vous ne pouvez pas utiliser un point d'accès comme destination pour la réplication S3. Pour plus d'informations sur la réplication, consultez Réplication d'objets au sein des régions et entre elles.
- Vous ne pouvez pas utiliser les alias de point d'accès S3 comme source ou destination pour les opérations Déplacer dans la console Amazon S3.
- Vous ne pouvez adresser les points d'accès qu'en utilisant virtual-host-style URLs. Pour plus d'informations sur l' virtual-host-styleadressage, consultezAccès à un compartiment à usage général Amazon S3.
- Les opérations d'API qui contrôlent la fonctionnalité des points d'accès (par exemple, `PutAccessPoint` et `GetAccessPointPolicy`) ne prennent pas en charge les appels intercomptes.
- Vous devez utiliser AWS la version 4 de Signature lorsque vous envoyez des demandes à un point d'accès à l'aide du REST APIs. Pour plus d'informations sur l'authentification des demandes, consultez Authentification des demandes (AWS Signature version 4) dans le manuel Amazon Simple Storage Service API Reference.
- Les points d'accès prennent uniquement en charge les demandes via HTTPS. Amazon S3 répond automatiquement par une redirection HTTP pour toutes les demandes effectuées via HTTP afin de les mettre à niveau vers HTTPS.
- Les points d'accès ne prennent pas en charge l'accès anonyme.
- Après avoir créé un point d'accès, vous ne pouvez pas modifier ses paramètres de blocage de l'accès public.
- Les points d'accès intercompte n'accordent pas l'accès aux données tant que vous n'avez pas obtenu les autorisations du propriétaire du compartiment. Le propriétaire du compartiment conserve toujours le contrôle ultime sur l'accès aux données et doit mettre à jour la politique du compartiment pour autoriser les demandes provenant du point d'accès intercompte. Pour afficher un exemple de politique de compartiment, consultez Configuration des politiques IAM pour l'utilisation des points d'accès.
- Régions AWS Lorsque vous avez plus de 1 000 points d'accès, vous ne pouvez pas rechercher un point d'accès par son nom dans la console Amazon S3.

- Lorsque vous consultez un point d'accès intercompte dans la console Amazon S3, la colonne Accès affiche Inconnu. La console Amazon S3 ne peut pas déterminer si un accès public est accordé au compartiment et aux objets associés. À moins que vous n'ayez besoin dune configuration publique pour un cas d'utilisation spécifique, nous vous recommandons, ainsi qu'au propriétaire du compartiment, de bloquer tout accès public au point d'accès et au compartiment. Pour de plus amples informations, veuillez consulter Blocage de l'accès public à votre stockage Amazon S3.

Restrictions et limitations relatives aux points d'accès associés à un volume sur un système de FSx fichiers Amazon

Les limites suivantes sont spécifiques à l'utilisation de points d'accès attachés à un volume sur un système de FSx fichiers Amazon :

- Lorsque vous créez un point d'accès, vous ne pouvez associer le point d'accès qu'à un volume sur un système de FSx fichiers Amazon dont vous êtes le propriétaire. Vous ne pouvez pas vous connecter à un volume appartenant à un autre Compte AWS.
- Vous ne pouvez pas utiliser l'`CreateAccessPoint`API lors de la création et de l'attachement d'un point d'accès à un volume sur un système de FSx fichiers Amazon. Vous devez utiliser l'CreateAndAttachS3AccessPointAPI.
- Vous ne pouvez désactiver aucun paramètre de blocage de l'accès public lors de la création ou de l'utilisation d'un point d'accès attaché à un volume sur un système de FSx fichiers Amazon.
- Vous ne pouvez pas répertorier des objets ni utiliser les opérations de copie ou de déplacement dans la console S3 avec des points d'accès attachés à un volume sur un système de FSx fichiers Amazon.
- `CopyObject`est pris en charge pour les points d'accès attachés à un FSx volume OpenZFS uniquement si la source et la destination sont le même point d'accès. Pour plus d'informations sur la compatibilité des points d'accès, consultezCompatibilité avec les points d'accès.
- Les téléchargements partitionnés sont limités à 5 Go.
- FSx pour OpenZFS, le type de déploiement et la prise en charge des classes de stockage varient en fonction de. Région AWS Pour plus d'informations, consultez la section Disponibilité par Région AWS dans le guide de l'utilisateur d'OpenZFS.

Référencement de points d'accès sous forme d' ARNsalias de point d'accès ou de type hébergé virtuellement URIs

Après avoir créé un point d'accès, vous pouvez utiliser ces points de terminaison pour effectuer un certain nombre d'opérations. Lorsque vous faites référence à un point d'accès, vous pouvez utiliser les Amazon Resource Names (ARNs), l'alias du point d'accès ou l'URI de type hébergé virtuel.

Rubriques

- Point d'accès ARNs
- Alias de point d'accès
- URI de style hébergé virtuellement

Point d'accès ARNs

Les points d'accès ont des noms de ressources Amazon (ARNs). ARNs Les points d'accès sont similaires aux compartiments ARNs, mais ils sont explicitement saisis et encodent le point d'accès Région AWS et l' Compte AWS ID du propriétaire du point d'accès. Pour plus d'informations ARNs, consultez la section Identifier les AWS ressources avec Amazon Resource Names (ARNs) dans le guide de l'utilisateur IAM.

Le point ARNs d'accès utilise le format suivant :

```
arn:aws:s3:region:account-id:accesspoint/resource
```

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test` représente le point d'accès nommé *`test`*, qui appartient au compte *`123456789012`* dans la région *`us-west-2`*.
- `arn:aws:s3:us-west-2:123456789012:accesspoint/*` représente tous les points d'accès du compte *`123456789012`* dans la région *`us-west-2`*.

ARNs pour les objets accessibles via un point d'accès, utilisez le format suivant :

```
arn:aws:s3:region:account-id:accesspoint/access-point-name/object/resource
```

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/unit-01` représente l'objet *`unit-01`*, accessible via le point d'accès nommé *`test`*, qui appartient au compte *`123456789012`* dans la région *`us-west-2`*.

- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/*` représente tous les objets du point d'accès nommé *test*, qui appartient au compte *123456789012* dans la région *us-west-2*.
- `arn:aws:s3:us-west-2:123456789012:accesspoint/test/object/unit-01/finance/*` représente tous les objets sous le préfixe *unit-01/finance/* pour le point d'accès nommé *test*, qui appartient au compte *123456789012* dans la région *us-west-2*.

Alias de point d'accès

Lorsque vous créez un point d'accès, Amazon S3 génère automatiquement un alias que vous pouvez utiliser pour l'accès aux données au lieu d'un nom de compartiment Amazon S3. Vous pouvez utiliser cet alias de point d'accès à la place d'un Amazon Resource Name (ARN) pour les opérations de plan de données de point d'accès. Pour obtenir la liste de ces opérations, consultez la page Compatibilité avec les points d'accès.

Un nom d'alias de point d'accès est créé dans le même espace de noms qu'un compartiment Amazon S3. Ce nom d'alias est généré automatiquement et ne peut pas être modifié. Un nom d'alias de point d'accès répond à toutes les exigences d'un nom de compartiment Amazon S3 valide et comprend les parties suivantes :

ACCESS POINT NAME`-METADATA-s3alias`(pour les points d'accès attachés à un compartiment Amazon S3)

ACCESS POINT NAME`-METADATA-ext-s3alias`(pour les points d'accès attachés à une source de données de compartiment autre que S3)

> **Note**
>
> Les `-ext-s3alias` suffixes `-s3alias` et sont réservés aux noms d'alias des points d'accès et ne peuvent pas être utilisés pour les noms de bucket ou de point d'accès. Pour plus d'informations sur les règles d'attribution de noms des compartiments Amazon S3, consultez Règles de dénomination des compartiments à usage général.

Points d'accès, alias, cas d'utilisation et limites

Lorsque vous adoptez des points d'accès, vous pouvez utiliser des noms d'alias de point d'accès sans nécessiter d'importantes modifications du code.

Lorsque vous créez un point d'accès, Amazon S3 génère automatiquement un nom d'alias de point d'accès, comme illustré dans l'exemple suivant. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control create-access-point --bucket amzn-s3-demo-bucket1 --name my-access-point
 --account-id 111122223333
{
    "AccessPointArn": "arn:aws:s3:region:111122223333:accesspoint/my-access-point",
    "Alias": "my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-s3alias"
}
```

Vous pouvez utiliser ce nom d'alias de point d'accès plutôt qu'un nom de compartiment Amazon S3 pour toutes les opérations de plan de données. Pour obtenir la liste de ces opérations, veuillez consulter la page Compatibilité avec les points d'accès.

L' AWS CLI exemple de `get-object` commande suivant utilise l'alias du point d'accès du compartiment pour renvoyer des informations sur l'objet spécifié. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3api get-object --bucket my-access-point-aqfqprnstn7aefdfbarligizwgyfouse1a-
s3alias --key dir/my_data.rtf my_data.rtf

{
    "AcceptRanges": "bytes",
    "LastModified": "2020-01-08T22:16:28+00:00",
    "ContentLength": 910,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
    "VersionId": "null",
    "ContentType": "text/rtf",
    "Metadata": {}
}
```

Limitations relatives aux alias des points d'accès

- Les alias ne peuvent pas être configurés par les clients.
- Les alias ne peuvent pas être supprimés, modifiés ni désactivés sur un point d'accès.
- Vous pouvez utiliser ce nom d'alias de point d'accès à la place d'un nom de compartiment Amazon S3 dans certaines opérations de plan de données. Pour obtenir la liste de ces opérations, veuillez consulter la page Compatibilité des points d'accès avec les opérations S3.

- Vous ne pouvez pas utiliser un nom d'alias de point d'accès pour les opérations relatives au plan de contrôle Amazon S3. Pour obtenir la liste des opérations relatives au plan de contrôle Amazon S3, consultez Contrôle Amazon S3 dans la Référence des API Amazon Simple Storage Service.
- Vous ne pouvez pas utiliser les alias de point d'accès S3 comme source ou destination pour les opérations Déplacer dans la console Amazon S3.
- Les alias ne peuvent pas être utilisés dans les AWS Identity and Access Management politiques (IAM).
- Les alias ne peuvent pas être utilisés comme destination de journalisation pour les journaux d'accès au serveur S3.
- Les alias ne peuvent pas être utilisés comme destination de journalisation pour les journaux AWS CloudTrail .
- Amazon SageMaker AI GroundTruth ne prend pas en charge les alias de point d'accès.

URI de style hébergé virtuellement

Les points d'accès prennent uniquement en charge l' virtual-host-styleadressage. Dans un URI de type hébergé virtuellement, le nom du point d'accès Compte AWS, et Région AWS fait partie du nom de domaine de l'URL. Pour plus d'informations sur l'hébergement virtuel, consultezHébergement virtuel de buckets à usage général.

L'URI de type virtual-host pour les points d'accès utilise le format suivant :

```
https://access-point-name-account-id.s3-accesspoint.region.amazonaws.com
```

> **Note**
>
> - Si le nom de votre point d'accès inclut des tirets (-), incluez les tirets dans l'URL et insérez un autre tiret avant l'ID du compte. Par exemple, pour utiliser un point d'accès nommé *finance-docs* appartenant au compte *123456789012* dans la région *us-west-2*, l'URL appropriée serait `https://finance-docs-123456789012.s3-accesspoint.us-west-2.amazonaws.com`.
> - Les points d'accès S3 ne prennent pas en charge l'accès via HTTP. Les points d'accès prennent uniquement en charge l'accès sécurisé par HTTPS.

Compatibilité avec les points d'accès

Vous pouvez utiliser des points d'accès pour accéder à des objets à l'aide du sous-ensemble suivant d'Amazon S3 APIs. Toutes les opérations répertoriées ci-dessous peuvent accepter des points d'accès ARNs ou des alias de point d'accès.

Pour des exemples d'utilisation de points d'accès pour effectuer des opérations sur des objets, reportez-vous àUtilisation des points d'accès Amazon S3 pour des compartiments à usage général.

Compatibilité des points d'accès avec les opérations S3

Le tableau suivant présente une liste partielle des opérations Amazon S3 et indique si elles sont compatibles avec les points d'accès. Toutes les opérations ci-dessous sont prises en charge par les points d'accès utilisant un compartiment S3 comme source de données, tandis que seules certaines opérations sont prises en charge par les points d'accès utilisant un volume FSx pour OpenZFS comme source de données.

Pour plus d'informations, consultez la section Compatibilité des points d'accès dans le guide de l'utilisateur FSx pour OpenZFS.

Fonctionnement S3	Point d'accès connecté à un compartiment S3	Point d'accès attaché à un volume FSx pour OpenZFS
AbortMultipartUpload	Pris en charge	Pris en charge
CompleteMultipartUpload	Pris en charge	Pris en charge
CopyObject (copies dans une même région uniquement)	Pris en charge	Pris en charge, si la source et la destination sont le même point d'accès
CreateMultipartUpload	Pris en charge	Pris en charge
DeleteObject	Pris en charge	Pris en charge
DeleteObjects	Pris en charge	Pris en charge
DeleteObjectTagging	Pris en charge	Pris en charge

Fonctionnement S3	Point d'accès connecté à un compartiment S3	Point d'accès attaché à un volume FSx pour OpenZFS
GetBucketAcl	Pris en charge	Non pris en charge
GetBucketCors	Pris en charge	Non pris en charge
GetBucketLocation	Pris en charge	Pris en charge
GetBucketNotificationConfiguration	Pris en charge	Non pris en charge
GetBucketPolicy	Pris en charge	Non pris en charge
GetObject	Pris en charge	Pris en charge
GetObjectAcl	Pris en charge	Non pris en charge
GetObjectAttributes	Pris en charge	Pris en charge
GetObjectLegalHold	Pris en charge	Non pris en charge
GetObjectRetention	Pris en charge	Non pris en charge
GetObjectTagging	Pris en charge	Pris en charge
HeadBucket	Pris en charge	Pris en charge
HeadObject	Pris en charge	Pris en charge
ListMultipartUploads	Pris en charge	Pris en charge
ListObjects	Pris en charge	Pris en charge
ListObjectsV2	Pris en charge	Pris en charge
ListObjectVersions	Pris en charge	Non pris en charge
ListParts	Pris en charge	Pris en charge
Presign	Pris en charge	Pris en charge

Fonctionnement S3	Point d'accès connecté à un compartiment S3	Point d'accès attaché à un volume FSx pour OpenZFS
PutObject	Pris en charge	Pris en charge
PutObjectAcl	Pris en charge	Non pris en charge
PutObjectLegalHold	Pris en charge	Non pris en charge
PutObjectRetention	Pris en charge	Non pris en charge
PutObjectTagging	Pris en charge	Pris en charge
RestoreObject	Pris en charge	Non pris en charge
UploadPart	Pris en charge	Pris en charge
UploadPartCopy (copies dans une même région uniquement)	Pris en charge	Pris en charge, si la source et la destination sont le même point d'accès

Configuration des politiques IAM pour l'utilisation des points d'accès

Les points d'accès Amazon S3 prennent en charge les politiques de ressources AWS Identity and Access Management (IAM) qui vous permettent de contrôler l'utilisation du point d'accès par ressource, par utilisateur ou selon d'autres conditions. Pour qu'une application ou un utilisateur puisse accéder à des objets via un point d'accès, le point d'accès et le bucket sous-jacent ou le système de FSx fichiers Amazon doivent autoriser la demande.

> **Important**
>
> Les restrictions que vous incluez dans une stratégie de point d'accès s'appliquent uniquement aux demandes effectuées via ce point d'accès. L'attachement d'un point d'accès à un bucket ne modifie pas le comportement de la ressource sous-jacente. Toutes les opérations existantes sur le bucket qui n'ont pas été effectuées via votre point d'accès continueront de fonctionner comme avant.

Lorsque vous utilisez des politiques de ressources IAM, veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions AWS Identity and Access Management Access Analyzer avant d'enregistrer votre politique. IAM Access Analyzer exécute des vérifications de politiques pour valider votre politique par rapport à la grammaire de politique et aux bonnes pratiques IAM. Ces vérifications génèrent des résultats et fournissent des recommandations pour vous aider à créer des stratégies fonctionnelles et conformes aux bonnes pratiques en matière de sécurité.

Pour en savoir plus sur la validation des politiques à l'aide d'IAM Access Analyzer, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM. Pour afficher la liste des avertissements, erreurs et suggestions renvoyés par IAM Access Analyzer, consultez la Référence de vérification de politique IAM Access Analyzer.

Exemples de politiques pour les points d'accès

Les exemples suivants montrent comment créer des politiques IAM pour contrôler les demandes effectuées via un point d'accès.

> **Note**
>
> Les autorisations accordées dans une politique de point d'accès ne sont effectives que si le compartiment sous-jacent autorise également le même accès. Vous pouvez y parvenir de deux façons :
>
> 1. (Recommandé) Déléguer le contrôle d'accès du compartiment au point d'accès, comme décrit à la section Délégation du contrôle d'accès aux points d'accès.
> 2. Ajoutez les mêmes autorisations contenues dans la stratégie de point d'accès à la stratégie du compartiment sous-jacent. Le premier exemple de politique de point d'accès montre comment modifier la politique de compartiment sous-jacente pour autoriser l'accès nécessaire.

Example 1 : octroi de politique de point d'accès

La politique de point d'accès suivante accorde à l'utilisateur IAM *Jane* dans le compte *123456789012* des autorisations GET et PUT pour des objets avec le préfixe *Jane/* via le point d'accès *my-access-point* dans le compte *123456789012*.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Jane"
        },
        "Action": ["s3:GetObject", "s3:PutObject"],
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-point/object/Jane/*"
    }]
}
```

Note

Pour que la stratégie de point d'accès accorde effectivement l'accès à *Jane*, il faut que le compartiment sous-jacent autorise également le même accès à *Jane*. Vous pouvez déléguer le contrôle d'accès du compartiment au point d'accès comme décrit à la section Délégation du contrôle d'accès aux points d'accès. Vous pouvez également ajouter la stratégie suivante au compartiment sous-jacent pour accorder les autorisations nécessaires à Jane. Notez que l'entrée `Resource` diffère entre les stratégies de point d'accès et de compartiment.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Jane"
        },
        "Action": ["s3:GetObject", "s3:PutObject"],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/Jane/*"
    }]
```

```
}
```

Example 2 : politique de point d'accès avec condition d'étiquette

La politique de point d'accès suivante accorde à l'utilisateur IAM *Mateo* dans le compte *123456789012* des autorisations pour des objets GET via le point d'accès *my-access-point* du compte *123456789012* dont la valeur de la clé d'étiquette *data* est définie sur *finance*.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect":"Allow",
        "Principal" : {
            "AWS": "arn:aws:iam::123456789012:user/Mateo"
        },
        "Action":"s3:GetObject",
        "Resource" : "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-
point/object/*",
        "Condition" : {
            "StringEquals": {
                "s3:ExistingObjectTag/data": "finance"
            }
        }
    }]
}
```

Example 3 : politique de point d'accès permettant d'établir la liste des compartiments

La politique de point d'accès suivante permet à l'utilisateur IAM `Arnav` dans le compte *123456789012* d'afficher les objets contenus dans le point d'accès sous-jacent du compartiment *my-access-point* dans le compte *123456789012*.

JSON

```
{
```

```
    "Version":"2012-10-17",
    "Statement": [
    {
        "Effect": "Allow",
        "Principal": {
            "AWS": "arn:aws:iam::123456789012:user/Arnav"
        },
        "Action": "s3:ListBucket",
        "Resource": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-access-
point"
    }]
}
```

Example 4 : politique de contrôle des services

La stratégie de contrôle de service suivante exige que tous les nouveaux points d'accès soient créés avec une origine de réseau de cloud privé virtuel (VPC). Lorsque cette stratégie est mise en place, les utilisateurs de votre organisation ne peuvent pas créer de nouveaux points d'accès accessibles à partir d'Internet.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Effect": "Deny",
        "Action": "s3:CreateAccessPoint",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "s3:AccessPointNetworkOrigin": "VPC"
            }
        }
    }]
}
```

Example 5 : politique de compartiment pour limiter les opérations S3 aux origines réseau VPC

La politique de compartiment suivante limite l'accès à toutes les opérations d'objet S3 pour le compartiment *amzn-s3-demo-bucket* aux points d'accès ayant une origine réseau VPC.

> **Important**
>
> Avant d'utiliser une instruction comme celle présentée dans cet exemple, assurez-vous que vous n'avez pas besoin d'utiliser des fonctions qui ne sont pas prises en charge par les points d'accès, comme la réplication entre régions.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:BypassGovernanceRetention",
                "s3:DeleteObject",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersion",
                "s3:DeleteObjectVersionTagging",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectVersionTagging",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl",
                "s3:PutObjectLegalHold",
                "s3:PutObjectRetention",
                "s3:PutObjectTagging",
                "s3:PutObjectVersionAcl",
```

```
                "s3:PutObjectVersionTagging",
                "s3:RestoreObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:AccessPointNetworkOrigin": "VPC"
                }
            }
        }
    ]
}
```

Clés de condition

Les points d'accès S3 comportent des clés de condition que vous pouvez utiliser dans les politiques IAM pour contrôler l'accès à vos ressources. Les clés de condition suivantes ne représentent qu'une partie d'une politique IAM. Pour obtenir des exemples complets de politiques, consultez Exemples de politiques pour les points d'accès, the section called "Délégation du contrôle d'accès aux points d'accès" et the section called "Octroi d'autorisations pour les points d'accès intercompte".

`s3:DataAccessPointArn`

Cet exemple présente une chaîne que vous pouvez utiliser pour établir une correspondance sur un ARN de point d'accès. L'exemple suivant correspond à tous les points d'accès Compte AWS *123456789012* de la région *us-west-2* :

```
"Condition" : {
    "StringLike": {
        "s3:DataAccessPointArn": "arn:aws:s3:us-west-2:123456789012:accesspoint/*"
    }
}
```

`s3:DataAccessPointAccount`

Cet exemple présente un opérateur de chaîne que vous pouvez utiliser pour établir une correspondance sur l'ID de compte du propriétaire d'un point d'accès. L'exemple suivant correspond à tous les points d'accès appartenant au Compte AWS *123456789012*.

```
"Condition" : {
    "StringEquals": {
```

```
        "s3:DataAccessPointAccount": "123456789012"
    }
}
```

`s3:AccessPointNetworkOrigin`

Cet exemple présente un opérateur de chaîne que vous pouvez utiliser pour faire correspondre sur l'origine du réseau, soit `Internet`, soit `VPC`. L'exemple suivant ne correspond qu'aux points d'accès ayant une origine VPC.

```
"Condition" : {
    "StringEquals": {
        "s3:AccessPointNetworkOrigin": "VPC"
    }
}
```

Pour plus d'informations sur l'utilisation des clés de condition avec Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Délégation du contrôle d'accès aux points d'accès

Vous pouvez déléguer le contrôle d'accès à un compartiment aux points d'accès du compartiment. Dans l'exemple suivant, la politique de compartiment permet un accès complet à tous les points d'accès appartenant au compte du propriétaire du compartiment. Ainsi, tous les accès à ce compartiment sont contrôlés par les stratégies attachées à ses points d'accès. Nous vous recommandons de configurer vos compartiments de cette façon pour tous les cas d'utilisation qui ne demandent pas d'accès direct au compartiment.

Example 6 : politique de compartiment qui délègue le contrôle d'accès aux points d'accès

JSON

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

```
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "arn:aws:s3:::amzn-s3-demo-bucket", "arn:aws:s3:::amzn-s3-
demo-bucket/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "111122223333" }
        }
    }]
}
```

Octroi d'autorisations pour les points d'accès intercompte

Pour créer un point d'accès à un compartiment qui appartient à un autre compte, vous devez d'abord créer le point d'accès en spécifiant le nom du compartiment et l'ID du propriétaire du compte. Ensuite, le propriétaire du compartiment doit mettre à jour la politique de compartiment pour autoriser les requêtes du point d'accès. La création d'un point d'accès est similaire à la création d'un DNS CNAME dans la mesure où le point d'accès ne donne pas accès au contenu du compartiment. Tous les accès aux compartiments sont contrôlés par la politique des compartiments. L'exemple de politique de compartiment suivant autorise les requêtes `GET` et `LIST` sur le compartiment depuis un point d'accès appartenant à un Compte AWS de confiance.

*`Bucket ARN`*Remplacez-le par l'ARN du bucket.

Example 7 — Politique de compartiment déléguant des autorisations à un autre Compte AWS

JSON

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : ["s3:GetObject","s3:ListBucket"],
        "Resource" : ["arn:aws:s3:::amzn-s3-demo-bucket", "arn:aws:s3:::amzn-s3-
demo-bucket/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointAccount" : "Access point
 owner's account ID" }
        }
```

```
    }]
}
```

> **Note**
>
> Les points d'accès entre comptes ne sont disponibles que pour les points d'accès attachés aux compartiments S3. Vous ne pouvez pas associer un point d'accès à un volume sur un système de FSx fichiers Amazon appartenant à un autre Compte AWS.

Surveillance et journalisation des points d'accès

Amazon S3 journalise les demandes effectuées via les points d'accès et les demandes adressées aux opérations d'API qui gèrent les points d'accès, telles que `CreateAccessPoint` et `GetAccessPointPolicy`. Pour surveiller et gérer les modèles d'utilisation, vous pouvez également configurer les métriques de demande Amazon CloudWatch Logs pour les points d'accès.

Rubriques

- CloudWatch métriques de demande
- AWS CloudTrail journaux des demandes effectuées via les points d'accès

CloudWatch métriques de demande

Pour comprendre et améliorer les performances des applications qui utilisent des points d'accès, vous pouvez utiliser CloudWatch les métriques de demande Amazon S3. Les métriques de demandes vous aident à contrôler les demandes Amazon S3 pour identifier rapidement les problèmes opérationnels et agir en conséquence.

Par défaut, ces métriques de demandes sont disponibles au niveau du compartiment. Toutefois, vous pouvez définir un filtre pour les métriques de demande à l'aide d'un préfixe partagé, de balises d'objet ou d'un point d'accès. Lorsque vous créez un filtre de point d'accès, la configuration des métriques de demandes inclut les demandes vers le point d'accès que vous spécifiez. Ce point d'accès vous permet de recevoir les métriques, de définir les alarmes et d'accéder aux tableaux de bord pour afficher les opérations effectuées en temps réel.

Vous devez activer les métriques de demandes en les configurant dans la console ou en utilisant l'API Amazon S3. Ces métriques sont disponibles à des intervalles d'une minute après une latence

pour le traitement. Les métriques de demande sont facturées au même tarif que les métriques CloudWatch personnalisées. Pour plus d'informations, consultez les CloudWatch tarifs Amazon.

Pour créer une configuration de métriques de demandes qui filtre par point d'accès, consultez Création d'une configuration de métriques qui filtre par préfixe, balise d'objet ou point d'accès.

AWS CloudTrail journaux des demandes effectuées via les points d'accès

Vous pouvez enregistrer les demandes effectuées via les points d'accès et les demandes adressées aux points d'accès APIs qui gèrent les points d'accès, `GetAccessPointPolicy`, par exemple `CreateAccessPoint` et en utilisant la journalisation des accès au serveur et AWS CloudTrail.

CloudTrail les entrées du journal pour les demandes effectuées via les points d'accès incluent l'ARN du point d'accès dans la `resources` section du journal.

Par exemple, supposons que vous ayez la configuration suivante :

- Un compartiment nommé *`amzn-s3-demo-bucket1`* dans la Région *`us-west-2`* qui contient un objet *`my-image.jpg`*
- Un point d'accès nommé *`my-bucket-ap`* associé à *`amzn-s3-demo-bucket1`*
- Un Compte AWS identifiant de *`123456789012`*

L'exemple suivant montre la `resources` section d'une entrée de CloudTrail journal pour la configuration précédente :

```
"resources": [
        {"type": "AWS::S3::Object",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1/my-image.jpg"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::Bucket",
            "ARN": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        {"accountId": "123456789012",
            "type": "AWS::S3::AccessPoint",
            "ARN": "arn:aws:s3:us-west-2:123456789012:accesspoint/my-bucket-ap"
        }
    ]
```

Si vous utilisez un point d'accès rattaché à un volume sur un système de FSx fichiers Amazon, la `resources` section d'une entrée de CloudTrail journal aura un aspect différent. Par exemple :

```
"resources": [
        {
            "accountId": "123456789012",
            "type": "AWS::FSx::Volume",
            "ARN": "arn:aws:fsx:us-east-1:123456789012:volume/fs-0123456789abcdef9/
fsvol-01234567891112223"
        }
    ]
```

Pour plus d'informations sur les journaux d'accès au serveur S3, consultez Enregistrement de demandes avec journalisation des accès au serveur. Pour plus d'informations AWS CloudTrail, voir Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

Création d'un point d'accès

Vous pouvez créer des points d'accès S3 à l'aide de l'API REST AWS Management Console AWS SDKs, AWS Command Line Interface (AWS CLI) ou Amazon S3. Les points d'accès sont appelés points de terminaison réseau attachés à une source de données telle qu'un bucket ou un volume Amazon FSx pour OpenZFS.

Par défaut, vous pouvez créer jusqu'à 10 000 points d'accès par région pour chacun de vos Comptes AWS. Si vous avez besoin de plus de 10 000 points d'accès pour un seul compte dans une même région, vous pouvez demander une augmentation des quotas de service. Pour plus d'informations sur les quotas de service et la demande d'une augmentation, consultez AWS Service Quotas dans Références générales AWS.

Rubriques

- Création de points d'accès avec des compartiments S3
- Création de points d'accès avec Amazon FSx
- Création de points d'accès restreints à un virtual private cloud
- Gestion de l'accès public aux points d'accès pour les compartiments à usage général

Création de points d'accès avec des compartiments S3

Un point d'accès est associé à un seul compartiment Amazon S3 à usage général. Si vous souhaitez utiliser un bucket dans votre Compte AWS, vous devez d'abord en créer un. Pour en savoir plus sur la création des compartiments, consultez Création, configuration et utilisation de compartiments à usage général Amazon S3.

Vous pouvez également créer un point d'accès intercompte associé à un compartiment dans un autre compte Compte AWS, à condition de connaître le nom du compartiment et l'ID du compte du propriétaire du compartiment. Cependant, la création de points d'accès intercompte ne vous donne pas accès aux données du compartiment tant que vous n'avez pas obtenu les autorisations du propriétaire du compartiment. Le propriétaire du compartiment doit accorder au compte du propriétaire du point d'accès (votre compte) l'accès au compartiment par le biais de la stratégie du compartiment. Pour de plus amples informations, veuillez consulter Octroi d'autorisations pour les points d'accès intercompte.

Utilisation de la console S3

Créer un point d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un point d'accès. Le point d'accès doit être créé dans la même région que le bucket associé.
3. Dans le volet de navigation, choisissez Points d'accès.
4. Dans la page Points d'accès, choisissez Créer un point d'accès.
5. Dans le champ Nom du point d'accès, saisissez le nom que vous souhaitez pour le point d'accès. Pour en savoir plus sur l'attribution de noms aux points d'accès, consultez Règles de dénomination pour les points d'accès.
6. Pour Source de données, spécifiez le compartiment S3 que vous souhaitez utiliser avec le point d'accès.

   Pour utiliser un compartiment dans votre compte, sélectionnez Choisir un compartiment dans ce compte et saisissez ou recherchez le nom du compartiment.

   Pour utiliser un compartiment dans un autre compte Compte AWS, choisissez Spécifier un compartiment dans un autre compte, puis entrez l' Compte AWS ID et le nom du compartiment.

Si vous utilisez un bucket dans un autre endroit Compte AWS, le propriétaire du bucket doit mettre à jour la politique du bucket afin d'autoriser les demandes provenant du point d'accès. Pour un exemple de politique de compartiment, consultez Octroi d'autorisations pour les points d'accès intercompte.

> **Note**
>
> Pour plus d'informations sur l'utilisation d'un volume FSx pour OpenZFS comme source de données, consultez. Création de points d'accès avec Amazon FSx

7. Choisissez une origine réseau, Internet ou un cloud privé virtuel (VPC). Si vous choisissez le cloud privé virtuel (VPC), entrez l'ID VPC que vous souhaitez utiliser avec le point d'accès.

   Pour en savoir plus sur les origines réseau des points d'accès, veuillez consulter Création de points d'accès restreints à un virtual private cloud.

8. Sous Block Public Access settings for this Access Point (Blocage de l'accès public pour ce point d'accès), sélectionnez les paramètres de blocage de l'accès public que vous voulez appliquer au point d'accès. Tous les paramètres de blocage d'accès public sont activés par défaut pour les nouveaux points d'accès. Nous vous recommandons de garder tous les paramètres activés, sauf si vous savez que vous avez un besoin spécifique de désactiver l'un d'entre eux.

   > **Note**
   >
   > Après avoir créé un point d'accès, vous ne pouvez pas modifier ses paramètres de blocage de l'accès public.

   Pour en savoir plus sur l'utilisation du blocage de l'accès public Amazon S3 avec des points d'accès, consultez Gestion de l'accès public aux points d'accès pour les compartiments à usage général.

9. (Facultatif) Sous Access point policy (Stratégie de point d'accès) - facultatif, spécifiez la stratégie de point d'accès. Avant d'enregistrer votre politique, veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions. Pour en savoir plus sur la spécification d'une stratégie de point d'accès, consultez Exemples de politiques pour les points d'accès.

10. Choisissez Create access point (Créer un point d'accès).

En utilisant le AWS CLI

L'exemple de commande suivant crée un point d'accès nommé *example-ap* pour le compartiment *amzn-s3-demo-bucket* dans le compte *111122223333*. Pour créer le point d'accès, vous envoyez une requête à Amazon S3 qui spécifie les éléments suivants :

- Nom du point d'accès. Pour plus d'informations sur les règles d'attribution de noms, consultez the section called "Règles de dénomination pour les points d'accès".
- Le nom du compartiment auquel vous voulez associer le point d'accès.
- L'identifiant du Compte AWS compte propriétaire du point d'accès.

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket
```

Lorsque vous créez un point d'accès en utilisant un bucket dans un autre Compte AWS, incluez le `--bucket-account-id` paramètre. L'exemple de commande suivant crée un point d'accès dans le Compte AWS *111122223333*, en utilisant le compartiment *amzn-s3-demo-bucket2*, qui se trouve dans le Compte AWS *444455556666*.

```
aws s3control create-access-point --name example-ap --account-id 111122223333 --
bucket amzn-s3-demo-bucket --bucket-account-id 444455556666
```

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour créer un point d'accès. Pour plus d'informations, consultez CreateAccessPoint dans la Référence d'API Amazon Simple Storage Service.

Création de points d'accès avec Amazon FSx

Vous pouvez créer et associer un point d'accès à un volume FSx pour OpenZFS à l'aide de FSx la console Amazon ou de l' AWS CLI API. Une fois attaché, vous pouvez utiliser l'objet S3 APIs pour accéder aux données de votre fichier. Vos données continuent de résider dans le système de FSx fichiers Amazon et d'être directement accessibles pour vos charges de travail existantes. Vous continuez à gérer votre stockage en utilisant toutes les fonctionnalités de gestion du stockage FSx d'OpenZFS, notamment les sauvegardes, les instantanés, les quotas d'utilisateurs et de groupes et la compression.

Pour obtenir des instructions sur la création d'un point d'accès et son attachement à un volume FSx pour OpenZFS, voir Création d'un point d'accès dans le guide de l'utilisateur FSx pour OpenZFS.

Création de points d'accès restreints à un virtual private cloud

Lorsque vous créez un point d'accès, vous pouvez choisir de le rendre accessible depuis Internet, ou vous pouvez spécifier que toutes les demandes effectuées via ce point d'accès doivent provenir d'un cloud privé virtuel (VPC) spécifique. Un point d'accès accessible depuis Internet est dit avoir une origine réseau d'`Internet`. Il peut être utilisé de n'importe où sur Internet, sous réserve de toute autre restriction d'accès en place pour le point d'accès, la source de données sous-jacente et les ressources associées, telles que les objets demandés. Un point d'accès accessible uniquement à partir d'un VPC spécifié a une origine réseau de `VPC`, et Amazon S3 rejette toute demande adressée au point d'accès qui ne provient pas de ce VPC.

> **Important**
>
> Vous ne pouvez spécifier l'origine réseau d'un point d'accès qu'au moment de la création du point d'accès. Après avoir créé le point d'accès, vous ne pouvez pas modifier son origine réseau.

Pour limiter un point d'accès à un accès VPC uniquement, vous devez inclure le paramètre `VpcConfiguration` à la demande de création du point d'accès. Dans le paramètre `VpcConfiguration`, vous spécifiez l'ID de VPC que vous souhaitez pouvoir utiliser avec le point d'accès. Si une demande est effectuée via le point d'accès, elle doit provenir du VPC, car Amazon S3 la rejettera dans le cas contraire.

Vous pouvez récupérer l'origine réseau d'un point d'accès à l'aide de AWS CLI AWS SDKs, ou REST APIs. Si un point d'accès a une configuration VPC spécifiée, son origine réseau est `VPC`. Sinon, l'origine réseau du point d'accès est `Internet`.

Exemple : créer et restreindre un point d'accès à un identifiant VPC

L'exemple suivant crée un point d'accès nommé `example-vpc-ap` pour le compartiment *`amzn-s3-demo-bucket`* dans le compte `123456789012` qui autorise l'accès uniquement à partir du VPC `vpc-1a2b3c`. L'exemple vérifie ensuite que le nouveau point d'accès a une origine réseau de `VPC`.

AWS CLI

```
aws s3control create-access-point --name example-vpc-ap --account-id 123456789012 --
bucket amzn-s3-demo-bucket --vpc-configuration VpcId=vpc-1a2b3c
```

```
aws s3control get-access-point --name example-vpc-ap --account-id 123456789012

{
    "Name": "example-vpc-ap",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "VPC",
    "VpcConfiguration": {
        "VpcId": "vpc-1a2b3c"
    },
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2019-11-27T00:00:00Z"
}
```

Pour utiliser un point d'accès avec un VPC, vous devez modifier la stratégie d'accès pour votre point de terminaison d'un VPC. Les points de terminaison d'un VPC autorisent la circulation du trafic de votre VPC vers Amazon S3. Ils disposent de politiques de contrôle d'accès qui contrôlent la façon dont les ressources du VPC sont autorisées à interagir avec Amazon S3. Les demandes de votre VPC vers Amazon S3 ne réussissent via un point d'accès que si la politique de point de terminaison d'un VPC accorde l'accès au point d'accès et au compartiment sous-jacent.

> **Note**
>
> Pour rendre les ressources accessibles uniquement au sein d'un VPC, veillez à créer une zone hébergée privée pour votre point de terminaison de VPC. Pour utiliser une zone hébergée privée, modifiez les paramètres de votre VPC de sorte que les attributs de réseau VPC `enableDnsHostnames` et `enableDnsSupport` soient définis sur `true`.

L'exemple de déclaration de stratégie suivant configure un point de terminaison d'un VPC pour autoriser les appels à `GetObject` pour un compartiment nommé `awsexamplebucket1` et un point d'accès nommé `example-vpc-ap`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::awsexamplebucket1/*",
            "arn:aws:s3:us-west-2:123456789012:accesspoint/example-vpc-ap/object/
*"
        ]
    }]
}
```

> **Note**
>
> La déclaration `"Resource"` de cet exemple utilise un Amazon Resource Name (ARN) pour spécifier le point d'accès. Pour plus d'informations sur le point d'accès ARNs, consultezRéférencement de points d'accès sous forme d' ARNsalias de point d'accès ou de type hébergé virtuellement URIs.

Pour plus d'informations sur les stratégies de point de terminaison d'un VPC, consultez Stratégies de point de terminaison pour Amazon S3 dans le Guide de l'utilisateur Amazon Virtual Private Cloud.

Pour un didacticiel sur la création de points d'accès avec des points de terminaison VPC, consultez Gérer l'accès Amazon S3 avec des points de terminaison et des points d'accès VPC.

Exemple : créer et restreindre un point d'accès attaché à un volume FSx pour OpenZFS à un VPC ID

Vous pouvez créer un point d'accès qui est attaché à un volume FSx pour OpenZFS à l'aide de la FSx console Amazon ou de l' AWS CLI API. Une fois attaché, vous pouvez utiliser l'objet S3 APIs pour accéder aux données de votre fichier à partir d'un VPC spécifique.

Pour obtenir des instructions sur la création et la restriction d'un point d'accès attaché à un volume FSx pour OpenZFS, voir Création de points d'accès restreints à un cloud privé virtuel (VPC) dans le guide de l'utilisateur FSx pour OpenZFS.

Gestion de l'accès public aux points d'accès pour les compartiments à usage général

Les points d'accès Amazon S3 prennent en charge des paramètres de blocage de l'accès public indépendants pour chaque point d'accès. Lorsque vous créez un point d'accès, vous pouvez spécifier les paramètres de blocage d'accès public qui s'appliquent à ce point d'accès. Pour toute demande effectuée via un point d'accès, Amazon S3 évalue les paramètres de blocage d'accès public pour ce point d'accès, le compartiment sous-jacent et le compte du propriétaire du compartiment. Si l'un de ces paramètres indique que la demande doit être bloquée, Amazon S3 rejette la demande.

Pour plus d'informations sur le blocage de l'accès public S3, consultez Blocage de l'accès public à votre stockage Amazon S3.

> **Important**
>
> - Tous les paramètres de blocage d'accès public sont activés par défaut pour les points d'accès. Vous devez désactiver explicitement tous les paramètres que vous ne souhaitez pas utiliser lors de la création du point d'accès.
> - Vous ne pouvez désactiver aucun paramètre de blocage de l'accès public lors de la création ou de l'utilisation d'un point d'accès rattaché à un système de FSx fichiers Amazon.
> - Après avoir créé un point d'accès, vous ne pouvez pas modifier ses paramètres de blocage de l'accès public.

Example

Exemple : Créer un point d'accès avec des paramètres de blocage d'accès public personnalisés

Cet exemple montre comment créer un point d'accès nommé `example-ap` pour le compartiment *`amzn-s3-demo-bucket`* dans le compte `123456789012` avec des paramètres de blocage d'accès public non définis par défaut. L'exemple extrait ensuite la configuration du nouveau point d'accès pour vérifier ses paramètres de blocage d'accès public.

AWS CLI

```
aws s3control create-access-point --name example-ap --account-id
 123456789012 --bucket amzn-s3-demo-bucket--public-access-block-configuration
 BlockPublicAcls=false,IgnorePublicAcls=false,BlockPublicPolicy=true,RestrictPublicBuckets=t
```

```
aws s3control get-access-point --name example-ap --account-id 123456789012

{
    "Name": "example-ap",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": false,
        "IgnorePublicAcls": false,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2019-11-27T00:00:00Z"
}
```

Gestion de vos points d'accès Amazon S3 pour les compartiments à usage général

Cette section explique comment gérer vos points d'accès Amazon S3 pour des compartiments à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST. Pour plus d'informations sur la gestion des points d'accès attachés à un volume FSx pour OpenZFS, consultez la section Gestion de vos points d'accès Amazon S3 dans le guide de l'utilisateur FSx pour OpenZFS.

> **Note**
>
> Vous ne pouvez utiliser que des points d'accès pour effectuer des opérations sur des objets. Vous ne pouvez pas utiliser les points d'accès pour effectuer d'autres opérations Amazon S3, telles que la suppression de compartiments ou la création de configurations de réplication S3. Pour obtenir la liste complète des opérations S3 qui prennent en charge les points d'accès, consultez Compatibilité avec les points d'accès.

Rubriques

- Répertoriez vos points d'accès pour les buckets à usage général
- Afficher les détails de votre point d'accès pour les buckets à usage général
- Supprimer votre point d'accès pour un bucket à usage général

Répertoriez vos points d'accès pour les buckets à usage général

Cette section explique comment répertorier vos points d'accès pour les buckets à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST.

Utilisation de la console S3

Pour répertorier les points d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.

En utilisant le AWS CLI

L'`list-access-points`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour répertorier vos points d'accès.

La commande suivante répertorie les points d'accès pour Compte AWS *111122223333*.

```
aws s3control list-access-points --account-id 111122223333
```

La commande suivante répertorie les points Compte AWS *111122223333* d'accès associés au bucket*amzn-s3-demo-bucket*.

```
aws s3control list-access-points --account-id 111122223333 --bucket amzn-s3-demo-bucket
```

Pour plus d'informations et des exemples, consultez list-access-points dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour répertorier vos points d'accès. Pour plus d'informations, consultez ListAccessPoints dans la Référence d'API Amazon Simple Storage Service.

Afficher les détails de votre point d'accès pour les buckets à usage général

Cette section explique comment afficher les détails de votre point d'accès pour un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST.

Utilisation de la console S3

Pour consulter les détails de votre point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Sélectionnez l'onglet Propriétés pour afficher la source de données du point d'accès, l'ID de compte Région AWS, la date de création, l'origine du réseau, l'URI S3, l'ARN et l'alias du point d'accès sélectionné.
7. Sélectionnez l'onglet Autorisations pour afficher les paramètres de blocage de l'accès public et la politique de point d'accès pour le point d'accès sélectionné.

> **Note**
>
> Vous ne pouvez pas modifier les paramètres de blocage de l'accès public pour un point d'accès une fois celui-ci créé.

En utilisant le AWS CLI

L'`get-access-point`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour afficher les détails de votre point d'accès.

La commande suivante répertorie les détails du point d'accès *my-access-point* à Compte AWS *111122223333* associer au compartiment S3*amzn-s3-demo-bucket*.

```
aws s3control get-access-point --name my-access-point --account-id 111122223333
```

Exemple de sortie :

```
{
    "Name": "my-access-point",
    "Bucket": "amzn-s3-demo-bucket",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2016-08-29T22:57:52Z",
    "Alias": "my-access-point-u1ny6bhm7moymqx8cuon8o1g4mwikuse2a-s3alias",
    "AccessPointArn": "arn:aws:s3:Région AWS:111122223333:accesspoint/my-access-point",
    "Endpoints": {
        "ipv4": "s3-accesspoint.Région AWS.amazonaws.com",
        "fips": "s3-accesspoint-fips.Région AWS.amazonaws.com",
        "fips_dualstack": "s3-accesspoint-fips.dualstack.Région AWS.amazonaws.com",
        "dualstack": "s3-accesspoint.dualstack.Région AWS.amazonaws.com"
    },
    "BucketAccountId": "111122223333"
}
```

La commande suivante répertorie les détails du point d'accès *example-fsx-ap* pour Compte AWS *444455556666*. Ce point d'accès est rattaché à un système de FSx fichiers Amazon.

```
aws s3control get-access-point --name example-fsx-ap --account-id 444455556666
```

Exemple de sortie :

```
{
    "Name": "example-fsx-ap",
    "Bucket": "",
    "NetworkOrigin": "Internet",
    "PublicAccessBlockConfiguration": {
        "BlockPublicAcls": true,
        "IgnorePublicAcls": true,
        "BlockPublicPolicy": true,
        "RestrictPublicBuckets": true
    },
    "CreationDate": "2025-01-19T14:16:12Z",
    "Alias": "example-fsx-ap-qrqbyebjtsxorhhaa5exx6r3q7-ext-s3alias",
    "AccessPointArn": "arn:aws:s3:Région AWS:444455556666:accesspoint/example-fsx-ap",
    "Endpoints": {
        "ipv4": "s3-accesspoint.Région AWS.amazonaws.com",
        "fips": "s3-accesspoint-fips.Région AWS.amazonaws.com",
        "fips_dualstack": "s3-accesspoint-fips.dualstack.Région AWS.amazonaws.com",
        "dualstack": "s3-accesspoint.dualstack.Région AWS.amazonaws.com"
    },
    "DataSourceId": "arn:aws::fsx:Région AWS:444455556666:file-system/
fs-5432106789abcdef0/volume/vol-0123456789abcdef0",
    "DataSourceType": "FSX_OPENZFS"
}
```

Pour plus d'informations et des exemples, consultez get-access-point dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour afficher les détails de votre point d'accès. Pour plus d'informations, consultez GetAccessPoint dans la Référence d'API Amazon Simple Storage Service.

Supprimer votre point d'accès pour un bucket à usage général

Cette section explique comment supprimer votre point d'accès pour un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST.

Utilisation de la console S3

À supprimer pour vos points d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Sur la page Point d'accès, sélectionnez Supprimer pour supprimer le point d'accès que vous avez sélectionné.
7. Pour confirmer la suppression, saisissez le nom du point d'accès et choisissez Supprimer.

En utilisant le AWS CLI

L'`delete-access-point`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour supprimer votre point d'accès.

La commande suivante supprime le point d'accès *`my-access-point`* pour Compte AWS *`111122223333`*.

```
aws s3control delete-access-point --name my-access-point --account-id 111122223333
```

Pour plus d'informations et des exemples, consultez delete-access-point dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour afficher les détails de votre point d'accès. Pour plus d'informations, consultez DeleteAccessPoint dans la Référence d'API Amazon Simple Storage Service.

Utilisation des points d'accès Amazon S3 pour des compartiments à usage général

Les exemples suivants montrent comment utiliser des points d'accès pour des compartiments à usage général avec des opérations compatibles dans Amazon S3.

> **Note**
>
> S3 génère automatiquement des alias de point d'accès pour tous les points d'accès. Ces alias peuvent être utilisés partout où un nom de compartiment est utilisé pour effectuer des opérations au niveau de l'objet. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Vous ne pouvez utiliser les points d'accès que pour les buckets à usage général afin d'effectuer des opérations sur des objets. Vous ne pouvez pas utiliser les points d'accès pour effectuer d'autres opérations Amazon S3, telles que la modification ou la suppression de compartiments. Pour obtenir la liste complète des opérations S3 qui prennent en charge les points d'accès, consultez Compatibilité avec les points d'accès.

Rubriques

- Répertorier les objets via un point d'accès pour un bucket à usage général
- Télécharger un objet via un point d'accès pour un bucket à usage général
- Configurer des listes de contrôle d'accès (ACLs) via un point d'accès pour un bucket à usage général
- Télécharger un objet via un point d'accès pour un bucket à usage général
- Ajouter un ensemble de balises via un point d'accès pour un bucket à usage général
- Supprimer un objet via un point d'accès pour un bucket à usage général

Répertorier les objets via un point d'accès pour un bucket à usage général

Cette section explique comment répertorier vos objets via un point d'accès pour un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST.

Utilisation de la console S3

Pour répertorier vos objets via un point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Dans l'onglet Objets, vous pouvez afficher le nom des objets auxquels vous souhaitez accéder via le point d'accès. Lorsque vous utilisez le point d'accès, vous ne pouvez effectuer que les opérations d'objet permises par les autorisations du point d'accès.

> **Note**
>
> - La vue de la console affiche toujours tous les objets du compartiment. L'utilisation d'un point d'accès comme cette procédure le décrit limite les opérations que vous pouvez effectuer sur ces objets, mais pas si vous pouvez voir qu'ils existent dans le compartiment.
> - Le AWS Management Console ne prend pas en charge l'utilisation de points d'accès au cloud privé virtuel (VPC) pour accéder aux ressources du bucket. Pour accéder aux ressources du bucket depuis un point d'accès VPC, utilisez le REST AWS CLI AWS SDKs, ou Amazon S3. APIs

En utilisant le AWS CLI

L'`list-objects-v2`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour répertorier votre objet via un point d'accès.

La commande suivante répertorie les objets permettant d' Compte AWS *111122223333*utiliser le point d'accès*my-access-point*.

```
aws s3api list-objects-v2 --bucket arn:aws:s3:Région AWS:111122223333:accesspoint/my-access-point
```

> **Note**
>
> S3 génère automatiquement des alias de point d'accès pour tous les points d'accès. Ces alias peuvent être utilisés partout où un nom de compartiment est utilisé pour effectuer des opérations au niveau de l'objet. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Pour plus d'informations et des exemples, consultez list-access-points dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour répertorier vos points d'accès. Pour plus d'informations, consultez ListObjectsV2 dans la Référence d'API Amazon Simple Storage Service.

Télécharger un objet via un point d'accès pour un bucket à usage général

Cette section explique comment télécharger un objet via un point d'accès pour un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST.

Utilisation de la console S3

Pour télécharger un objet via un point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.

3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Dans l'onglet Objets, sélectionnez le nom de l'objet que vous souhaitez télécharger.
7. Choisissez Téléchargement.

En utilisant le AWS CLI

L'`get-object`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour télécharger un objet via un point d'accès.

La commande suivante télécharge l'objet `puppy.jpg` pour Compte AWS *111122223333* utiliser le point d'accès*my-access-point*. Vous devez inclure un`outfile`, qui est le nom de fichier de l'objet téléchargé, tel que*my_downloaded_image.jpg*.

```
aws s3api get-object --bucket arn:aws:s3:Région AWS:111122223333:accesspoint/my-access-point --key puppy.jpg my_downloaded_image.jpg
```

> **Note**
>
> S3 génère automatiquement des alias de point d'accès pour tous les points d'accès. Ces alias peuvent être utilisés partout où un nom de compartiment est utilisé pour effectuer des opérations au niveau de l'objet. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Pour plus d'informations et des exemples, consultez get-object dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour télécharger un objet via un point d'accès. Pour plus d'informations, consultez GetObject dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDK pour Python pour télécharger un objet via un point d'accès.

Python

Dans l'exemple suivant, le fichier nommé *hello.txt* est téléchargé pour le AWS compte à *111122223333* l'aide du point d'accès nomméMy-access-point.

```
import boto3
s3 = boto3.client('s3')
s3.download_file('arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point',
 'hello.txt', '/tmp/hello.txt')
```

Configurer des listes de contrôle d'accès (ACLs) via un point d'accès pour un bucket à usage général

Cette section explique comment configurer ACLs via un point d'accès un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL).

Utilisation de la console S3

Pour configurer ACLs via un point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Dans l'onglet Objets, sélectionnez le nom de l'objet pour lequel vous souhaitez configurer une ACL.
7. Sous l'onglet Autorisations, sélectionnez Modifier pour configurer l'ACL de l'objet.

> **Note**
>
> Actuellement, Amazon S3 ne prend pas en charge la modification des paramètres de blocage de l'accès public d'un point d'accès après que ce point d'accès a été créé.

En utilisant le AWS CLI

L'`put-object-acl`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour configurer les autorisations d'accès via un point d'accès à l'aide d'une ACL.

La commande suivante applique une ACL à un objet existant `puppy.jpg` via un point d'accès appartenant à Compte AWS *`111122223333`*.

```
aws s3api put-object-acl --bucket arn:aws:s3:Région AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --acl private
```

> **Note**
>
> S3 génère automatiquement des alias de point d'accès pour tous les points d'accès. Ces alias peuvent être utilisés partout où un nom de compartiment est utilisé pour effectuer des opérations au niveau de l'objet. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Pour plus d'informations et des exemples, consultez put-object-acl dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour configurer les autorisations d'accès via un point d'accès à l'aide d'une ACL. Pour plus d'informations, consultez PutObjectAcl dans la Référence d'API Amazon Simple Storage Service.

Télécharger un objet via un point d'accès pour un bucket à usage général

Cette section explique comment télécharger un objet via un point d'accès pour un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST.

Utilisation de la console S3

Pour télécharger un objet via un point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Sous l'onglet Objets, sélectionnez Télécharger.
7. Glissez et déposez les fichiers et dossiers que vous souhaitez télécharger ici, ou choisissez Ajouter des fichiers ou Ajouter un dossier.

   > **Note**
   >
   > La console Amazon S3 vous permet de charger des fichiers d'une taille maximale de 160 Go. Pour charger un fichier de plus de 160 Go, utilisez l'API REST AWS Command Line Interface (AWS CLI) ou Amazon S3. AWS SDKs

8. Pour modifier les autorisations de la liste de contrôle d'accès, choisissez Permissions (Autorisations).
9. Sous Access control list (ACL) (Liste de contrôle d'accès (ACL)), modifiez les autorisations.

   Pour plus d'informations sur les autorisations d'accès aux objets, consultez Utilisation de la console S3 pour définir des autorisations ACL pour un objet. Vous pouvez octroyer l'accès en lecture à vos objets au public (tout le monde) pour tous les fichiers que vous chargez. Cependant, nous recommandons de ne pas modifier le paramètre par défaut de l'accès public en lecture. L'octroi de l'accès en lecture public est applicable à un petit sous-ensemble de cas d'utilisation, comme lorsque des compartiments sont utilisés pour des sites web. Vous pouvez toujours modifier les autorisations de l'objet après l'avoir chargé.
10. Pour configurer d'autres propriétés supplémentaires, sélectionnez Properties (Propriétés).
11. Dans Classe de stockage, choisissez la classe de stockage des fichiers à charger.

Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

12. Pour mettre à jour les paramètres de chiffrement de vos objets, sous Server-side encryption settings (Paramètres de chiffrement côté serveur), procédez comme suit.

    a. Choisissez Specify an encryption key (Spécifier une clé de chiffrement).

    b. Sous Paramètres de chiffrement, choisissez Utiliser les paramètres du compartiment pour le chiffrement par défaut ou Ignorer les paramètres du compartiment pour le chiffrement par défaut.

    c. Si vous avez choisi Ignorer les paramètres du compartiment pour le chiffrement par défaut, vous devez configurer les paramètres de chiffrement suivants.

    - Pour chiffrer les fichiers chargés à l'aide des clés gérées par Amazon S3, choisissez Clé gérée par Amazon S3 (SSE-S3).

      Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

    - Pour chiffrer les fichiers téléchargés à l'aide des clés stockées dans AWS Key Management Service (AWS KMS), choisissez AWS Key Management Service key (SSE-KMS). Choisissez ensuite l'une des options suivantes pour CléAWS KMS :

      - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis sélectionnez votre Clé KMS dans la liste des clés disponibles.

        La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

      - Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN de votre clé KMS dans le champ qui apparaît.

      - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

        Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez d'abord avoir l'autorisation d'utiliser cette clé KMS, puis saisir l'ARN de la clé KMS.
>
> Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez la section Identifying symmetric and asymmetric KMS keys (Identification des clés KMS symétriques et asymétriques) dans le Guide du développeur AWS Key Management Service .

13. Pour utiliser des sommes de contrôle supplémentaires, sélectionnez Activé. Ensuite, pour le champ Checksum function (Fonction total de contrôle), sélectionnez la fonction que vous souhaitez utiliser. Amazon S3 calcule et stocke la valeur du total de contrôle après avoir reçu l'objet entier. Vous pouvez utiliser la case Precalculated value (Valeur précalculée) pour fournir une valeur précalculée. Si vous le faites, Amazon S3 compare la valeur que vous avez fournie à la valeur qu'il calcule. Si les deux valeurs ne correspondent pas, Amazon S3 génère une erreur.

    Les totaux de contrôle supplémentaires vous permettent de spécifier l'algorithme de total de contrôle que vous souhaitez utiliser pour vérifier vos données. Pour plus d'informations sur les totaux de contrôle supplémentaires, consultez Vérification de l'intégrité des objets dans Amazon S3.

14. Pour ajouter des balises à tous les objets que vous chargez, choisissez Add tag (Ajouter une balise). Saisissez un nom de balise dans le champ Clé. Saisissez une valeur pour la balise.

    Le balisage des objets vous permet de classer le stockage par catégorie. Chaque balise est une paire clés-valeurs. Les valeurs de clés et de balises sont sensibles à la casse. Vous pouvez avoir jusqu'à 10 balises par objet. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 255 caractères Unicode. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.

15. Pour ajouter des métadonnées, choisissez Add metadata (Ajouter des métadonnées).

a. Sous Type, choisissez System defined (Défini par le système) ou User defined (Défini par l'utilisateur).

   Pour les métadonnées définies par le système, vous pouvez sélectionner des en-têtes HTTP courants, tels que Content-Type et Content-Disposition. Pour obtenir la liste des métadonnées définies par le système et savoir si vous pouvez ajouter la valeur, consultez Métadonnées d'objet définies par le système. Toute métadonnée commençant par le préfixe `x-amz-meta-` est traitée comme une métadonnée définie par l'utilisateur. Les métadonnées définies par l'utilisateur sont stockées avec l'objet et renvoyées une fois que vous avez téléchargé l'objet. Les clés et leurs valeurs doivent respecter les normes US-ASCII. Les métadonnées définies par l'utilisateur peuvent atteindre 2 Ko. Pour plus d'informations sur les métadonnées définies par le système et par l'utilisateur, consultez Utilisation des métadonnées d'objet.

b. Pour Key (Clé), choisissez une clé.

c. Saisissez une valeur pour la clé.

16. Pour charger vos objets, choisissez Charger.

    Amazon S3 charge votre objet. Lorsque le chargement est terminé, un message de succès s'affiche sur la page Load: status (Charger : statut).

En utilisant le AWS CLI

L'`put-object`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour télécharger un objet via un point d'accès.

La commande suivante télécharge l'objet `puppy.jpg` pour Compte AWS *`111122223333`* utiliser le point *`my-access-point`* d'accès.

```
aws s3api put-object --bucket arn:aws:s3:Région AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --body puppy.jpg
```

> **Note**
>
> S3 génère automatiquement des alias de point d'accès pour tous les points d'accès et les alias de point d'accès peuvent être utilisés partout où un nom de compartiment est utilisé

pour effectuer des opérations au niveau de l'objet. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Pour plus d'informations et des exemples, consultez put-object dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour télécharger un objet via un point d'accès. Pour plus d'informations, consultez PutObject dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDK pour Python pour télécharger un objet via un point d'accès.

Python

Dans l'exemple suivant, le fichier nommé *hello.txt* est chargé pour le AWS compte à *111122223333* l'aide du point d'accès nommé*my-access-point*.

```
import boto3
s3 = boto3.client('s3')
s3.upload_file('/tmp/hello.txt', 'arn:aws:s3:us-east-1:111122223333:accesspoint/my-access-point', 'hello.txt')
```

Ajouter un ensemble de balises via un point d'accès pour un bucket à usage général

Cette section explique comment ajouter un ensemble de balises via un point d'accès pour un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST. Pour de plus amples informations, veuillez consulter Catégorisation de vos objets à l'aide de balises.

Utilisation de la console S3

Pour ajouter un ensemble de balises via un point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Dans l'onglet Objets, sélectionnez le nom de l'objet auquel vous souhaitez ajouter un ensemble de balises.
7. Dans l'onglet Propriétés, recherchez le sous-en-tête Tags et choisissez Modifier.
8. Passez en revue les objets répertoriés, puis choisissez Ajouter une étiquette.
9. Chaque balise d'objet est une paire clé-valeur. Saisissez une Key (Clé) et une Value (Valeur). Choisissez Add Tag (Ajouter une balise) pour ajouter une autre balise.

   Vous pouvez entrer jusqu'à 10 balises pour un objet.
10. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

L'`put-object-tagging`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour ajouter un ensemble de balises via un point d'accès.

La commande suivante ajoute un ensemble de balises pour un objet existant `puppy.jpg` utilisant un point d'accès. *`my-access-point`*

```
aws s3api put-object-tagging --bucket arn:aws:s3:Région
 AWS:111122223333:accesspoint/my-access-point --key puppy.jpg --tagging
 TagSet=[{Key="animal",Value="true"}]
```

> **Note**
>
> S3 génère automatiquement des alias de point d'accès pour tous les points d'accès et les alias de point d'accès peuvent être utilisés partout où un nom de compartiment est utilisé pour effectuer des opérations au niveau de l'objet. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Pour plus d'informations et des exemples, consultez put-object-tagging dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour ajouter un ensemble de balises à un objet via un point d'accès. Pour plus d'informations, consultez PutObjectTagging dans la Référence d'API Amazon Simple Storage Service.

Supprimer un objet via un point d'accès pour un bucket à usage général

Cette section explique comment supprimer un objet via un point d'accès pour un bucket à usage général à l'aide de l'API AWS Management Console AWS Command Line Interface, ou REST.

Utilisation de la console S3

Pour supprimer un ou plusieurs objets via un point d'accès dans votre Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région pour laquelle vous souhaitez afficher la liste des points d'accès.
3. Dans le volet de navigation sur le côté gauche de la console, choisissez Access Points.
4. (Facultatif) Recherchez les points d'accès par leur nom. Seuls les points d'accès que vous avez sélectionnés Région AWS apparaîtront ici.
5. Choisissez le nom du point d'accès que vous souhaitez gérer ou utiliser.
6. Dans l'onglet Objets, sélectionnez le nom de l'objet ou des objets que vous souhaitez supprimer.
7. Passez en revue les objets listés pour suppression, puis tapez delete dans la zone de confirmation.
8. Choisissez Supprimer les objets.

En utilisant le AWS CLI

L'`delete-object`exemple de commande suivant montre comment vous pouvez utiliser le AWS CLI pour supprimer un objet via un point d'accès.

La commande suivante supprime l'objet existant à l'`puppy.jpg`aide du point *`my-access-point`* d'accès.

```
aws s3api delete-object --bucket arn:aws:s3:Région AWS:111122223333:accesspoint/my-access-point --key puppy.jpg
```

> **Note**
>
> S3 génère automatiquement des alias de point d'accès pour tous les points d'accès et les alias de point d'accès peuvent être utilisés partout où un nom de compartiment est utilisé pour effectuer des opérations au niveau de l'objet. Pour de plus amples informations, veuillez consulter Alias de point d'accès.

Pour plus d'informations et des exemples, consultez delete-object dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour supprimer un objet via un point d'accès. Pour plus d'informations, consultez DeleteObject dans la Référence d'API Amazon Simple Storage Service.

Utilisation de balises avec des points d'accès S3 pour des compartiments à usage général

Une AWS balise est une paire clé-valeur qui contient des métadonnées sur les ressources, en l'occurrence les points d'accès Amazon S3. Vous pouvez étiqueter les points d'accès lorsque vous les créez ou gérer les balises sur les points d'accès existants. Pour des informations générales sur les balises, consultezMarquage pour la répartition des coûts ou le contrôle d'accès basé sur les attributs (ABAC).

> **Note**
>
> L'utilisation de balises sur les points d'accès est gratuite, au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3.

Méthodes courantes d'utilisation des balises avec les points d'accès

Le contrôle d'accès basé sur les attributs (ABAC) vous permet d'ajuster les autorisations d'accès et d'accorder l'accès aux points d'accès en fonction de leurs balises. Pour plus d'informations sur ABAC dans Amazon S3, consultez Utilisation de balises pour ABAC.

ABAC pour points d'accès S3

Les points d'accès Amazon S3 prennent en charge le contrôle d'accès basé sur les attributs (ABAC) à l'aide de balises. Utilisez des clés de condition basées sur des balises dans vos politiques AWS d'organisation, d'IAM et de points d'accès. Pour les entreprises, l'ABAC d'Amazon S3 prend en charge l'autorisation sur plusieurs AWS comptes.

Dans vos politiques IAM, vous pouvez contrôler l'accès aux points d'accès en fonction des balises des points d'accès à l'aide des clés de condition globales suivantes :

- `aws:ResourceTag/key-name`
  - Utilisez cette clé pour comparer la paire valeur clé d'étiquette que vous spécifiez dans la politique avec la paire valeur clé attachée à la ressource. Par exemple, vous pouvez exiger que l'accès à une ressource soit autorisé uniquement si la clé de balise `Dept` est attachée à la ressource avec la valeur `Marketing`. Pour plus d'informations, consultez la section Contrôle de l'accès aux AWS ressources.
- `aws:RequestTag/key-name`
  - Utilisez cette clé pour comparer la paire clé-valeur de balise qui a été transmise dans la demande avec la paire de balises spécifiée dans la politique. Par exemple, vous pouvez vérifier que la demande comprend la clé de balise `Dept` et qu'elle a la valeur `Accounting`. Pour plus d'informations, consultez la section Contrôle de l'accès lors AWS des demandes. Vous pouvez utiliser cette clé de condition pour restreindre les paires clé-valeur de balise qui peuvent être transmises pendant les opérations d'`CreateAccessPoint`API `TagResource` et d'API.
- `aws:TagKeys`
  - Utilisez cette clé pour comparer les clés de balise d'une demande avec celles spécifiées dans la politique. Nous vous recommandons, lorsque vous utilisez des politiques pour contrôler l'accès à l'aide de balises, d'utiliser la clé de condition `aws:TagKeys` pour définir quelles clés de balises sont autorisées. Pour des exemples de politiques et pour plus d'informations, consultez la section Contrôle de l'accès en fonction des clés de balise. Vous pouvez créer un point d'accès avec des balises. Pour autoriser le balisage pendant le fonctionnement de l'`CreateAccessPoint`API, vous devez créer une politique qui inclut à la fois les

`s3:CreateAccessPoint` actions `s3:TagResource` et. Vous pouvez ensuite utiliser la clé de `aws:TagKeys` condition pour appliquer l'utilisation de balises spécifiques dans la `CreateAccessPoint` demande.

- `s3:AccessPointTag/tag-key`
  - Utilisez cette clé de condition pour accorder des autorisations à des données spécifiques via des points d'accès utilisant des balises. Lors de l'utilisation `aws:ResourceTag/tag-key` dans le cadre d'une politique IAM, le point d'accès ainsi que le compartiment vers lequel le point d'accès pointe doivent avoir la même balise sont pris en compte lors de l'autorisation. Si vous souhaitez contrôler l'accès à vos données uniquement via la balise de point d'accès, vous pouvez utiliser la clé de `s3:AccessPointTag/tag-key` condition.

Exemple de politiques ABAC pour les points d'accès

Consultez les exemples de politiques ABAC suivants pour les points d'accès Amazon S3.

1.1 - Politique IAM pour créer ou modifier des buckets avec des balises spécifiques

Dans cette stratégie IAM, les utilisateurs ou les rôles dotés de cette politique ne peuvent créer des points d'accès que s'ils balisent les points d'accès avec la clé de balise `project` et la valeur de balise `Trinity` dans la demande de création de points d'accès. Ils peuvent également ajouter ou modifier des balises sur les points d'accès existants tant que la `TagResource` demande inclut la paire clé-valeur de la balise. `project:Trinity`

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAccessPointWithTags",
      "Effect": "Allow",
      "Action": [
        "s3:CreateAccessPoint",
        "s3:TagResource"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/project": [
            "Trinity"
          ]
        }
```

```
      }
    }
  ]
}
```

1.2 - Politique du point d'accès visant à restreindre les opérations sur le point d'accès à l'aide de balises

Dans cette politique de point d'accès, les principaux IAM (utilisateurs et rôles) peuvent effectuer des opérations à l'aide de l'`GetObject`action sur le point d'accès uniquement si la valeur de la `project` balise du point d'accès correspond à la valeur de la balise du `project` principal.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowObjectOperations",
      "Effect": "Allow",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        }
      }
    }
  ]
}
```

1.3 - Politique IAM visant à modifier les balises sur les ressources existantes tout en maintenant la gouvernance du balisage

Dans cette politique IAM, les principaux IAM (utilisateurs ou rôles) peuvent modifier les balises d'un point d'accès uniquement si la valeur de la `project` balise du point d'accès correspond à la valeur de la balise du principal. `project` Seules les quatre balises`project`, `environment``owner`, et `cost-center` spécifiées dans les clés de `aws:TagKeys` condition sont autorisées pour ces points d'accès. Cela permet de renforcer la gouvernance des balises, d'empêcher les modifications non

autorisées des balises et de garantir la cohérence du schéma de balisage sur l'ensemble de vos points d'accès.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "EnforceTaggingRulesOnModification",
      "Effect": "Allow",
      "Action": [
        "s3:TagResource"
      ],
      "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/project": "${aws:PrincipalTag/project}"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "project",
            "environment",
            "owner",
            "cost-center"
          ]
        }
      }
    }
  ]
}
```

1.4 - Utilisation de la clé de AccessPointTag condition s3 :

Dans cette politique IAM, l'énoncé de condition autorise l'accès aux données du bucket si le point d'accès possède la clé de balise `Environment` et la valeur `Production` de balise.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
```

```
      "Condition": {
        "StringEquals": {
          "s3:AccessPointTag/Environment": "Production"
        }
      }
    }
  ]
}
```

1.5 - Utilisation d'une politique de délégation de compartiments

Dans Amazon S3, vous pouvez déléguer l'accès ou le contrôle de votre politique de compartiment S3 à un autre AWS compte, à un utilisateur ou à un rôle spécifique AWS Identity and Access Management (IAM) dans l'autre compte. La politique de compartiment délégué accorde à cet autre compte, utilisateur ou rôle l'autorisation d'accéder à votre compartiment et à ses objets. Pour plus d'informations, consultez la section Délégation d'autorisations.

Si vous utilisez une politique de compartiment délégué, telle que la suivante :

```
{
  "Version": "2012-10-17",
    "Statement": {
      "Principal": {"AWS": "*"},
        "Effect": "Allow",
        "Action": ["s3:*"],
        "Resource":["arn:aws::s3:::amzn-s3-demo-bucket/*", "arn:aws::s3:::amzn-s3-demo-
bucket"],
           "Condition": {
             "StringEquals" : {
                "s3:DataAccessPointAccount" : "111122223333"
             }
           }
    }
}
```

Dans la politique IAM suivante, l'énoncé de condition autorise l'accès aux données du bucket si le point d'accès possède la clé de balise `Environment` et la valeur `Production` de balise.

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

```
      "Sid": "AllowAccessToSpecificAccessPoint",
      "Effect": "Allow",
      "Action": "*",
      "Resource": "arn:aws::s3:region:111122223333:accesspoint/my-access-point",
      "Condition": {
        "StringEquals": {
          "s3:AccessPointTag/Environment": "Production"
        }
      }
    }
  ]
}
```

Utilisation de balises pour les points d'accès pour les compartiments à usage général

Vous pouvez ajouter ou gérer des balises pour les points d'accès à l'aide de la console Amazon S3, de l'interface de ligne de AWS commande (CLI) ou du S3 APIs : TagResourceUntagResource, et ListTagsForResource. AWS SDKs Pour plus d'informations, consultez :

Rubriques

- Création de points d'accès avec des tags
- Ajouter un tag à un point d'accès
- Afficher les balises des points d'accès
- Supprimer un tag d'un point d'accès

Création de points d'accès avec des tags

Vous pouvez étiqueter les points d'accès lorsque vous les créez. L'utilisation de balises sur les points d'accès est gratuite, au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3. Pour plus d'informations sur le balisage des points d'accès, consultezUtilisation de balises avec des points d'accès S3 pour des compartiments à usage général.

Autorisations

Pour créer un point d'accès avec des balises, vous devez disposer des autorisations suivantes :

- `s3:CreateBucket`
- `s3:TagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de créer un point d'accès avec des balises, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des éléments nécessaires Autorisations pour créer le point d'accès et y ajouter une étiquette.
- Vérifiez votre politique utilisateur IAM pour connaître les conditions de contrôle d'accès basé sur les attributs (ABAC). Il se peut que vous deviez étiqueter vos points d'accès uniquement avec des clés et des valeurs de balise spécifiques. Pour de plus amples informations, veuillez consulter Utilisation de balises pour le contrôle d'accès basé sur les attributs (ABAC).

Étapes

Vous pouvez créer un point d'accès avec des balises appliquées à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour créer un point d'accès avec des balises à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (General Purpose Buckets).
3. Choisissez Créer un point d'accès pour créer un nouveau point d'accès.
4. Sur la page Créer un point d'accès, l'option Tags est disponible lors de la création d'un nouveau point d'accès.
5. Entrez un nom pour le point d'accès. Pour de plus amples informations, veuillez consulter Règles, restrictions et limitations de dénomination des points d'accès.
6. Choisissez Ajouter une nouvelle balise pour ouvrir l'éditeur de balises et entrez une paire clé-valeur de balise. La clé de balise est obligatoire, mais la valeur est facultative.
7. Pour ajouter une autre étiquette, sélectionnez à nouveau Ajouter une nouvelle étiquette. Vous pouvez saisir jusqu'à 50 paires clé-valeur de balise.
8. Après avoir défini les options pour votre nouveau point d'accès, choisissez Create access point.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment créer un point d'accès avec des balises à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
CreateAccessPointRequest createAccessPointRequest =
 CreateAccessPointRequest.builder()
                .accountId(111122223333)
                .name(my-access-point)
                .bucket(amzn-s3-demo-bucket)

 .tags(Collections.singletonList(Tag.builder().key("key1").value("value1").build()))
                .build();
 awss3Control.createAccessPoint(createAccessPointRequest);
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la création d'un point d'accès avec des balises, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- CreateAccessPoint

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant vous montre comment créer un point d'accès avec des balises à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control create-access-point --name my-access-point \
--bucket amzn-s3-demo-bucket \
--account-id 111122223333 \ --profile personal \
```

```
--tags [{Key=key1,Value=value1},{Key=key2,Value=value2}] \
--region region
```

Ajouter un tag à un point d'accès

Vous pouvez ajouter des balises aux points d'accès Amazon S3 et modifier ces balises. L'utilisation de balises sur les points d'accès est gratuite, au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3. Pour plus d'informations sur le balisage des points d'accès, consultezUtilisation de balises avec des points d'accès S3 pour des compartiments à usage général.

Autorisations

Pour ajouter un tag à un point d'accès, vous devez disposer des autorisations suivantes :

- `s3:TagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez d'ajouter une balise à un point d'accès, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des conditions requises Autorisations pour ajouter une étiquette à un point d'accès.
- Si vous avez essayé d'ajouter une clé de balise commençant par le préfixe AWS réservé`aws:`, modifiez la clé de balise et réessayez.

Étapes

Vous pouvez ajouter des balises aux points d'accès à l'aide de la console Amazon S3, de l'interface de ligne de AWS commande (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour ajouter des balises à un point d'accès à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (General Purpose Buckets).
3. Choisissez le nom du point d'accès.

4. Choisissez l'onglet Propriétés.
5. Accédez à la section Tags et choisissez Ajouter un nouveau tag.
6. Cela ouvre la page Ajouter des balises. Vous pouvez saisir jusqu'à 50 paires clé-valeur de balise.
7. Si vous ajoutez une nouvelle balise portant le même nom de clé qu'une balise existante, la valeur de la nouvelle balise remplace la valeur de la balise existante.
8. Vous pouvez également modifier les valeurs des balises existantes sur cette page.
9. Après avoir ajouté les balises, choisissez Enregistrer les modifications.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment ajouter des balises à un point d'accès à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
TagResourceRequest tagResourceRequest =
 TagResourceRequest.builder().resourceArn(arn:aws::s3:region:111122223333:accesspoint/
my-access-point/*)
.accountId(111122223333)
.tags(List.of(Tag.builder().key("key1").value("value1").build(),
Tag.builder().key("key2").value("value2").build()))
.build();
awss3Control.tagResource(tagResourceRequest);
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour l'ajout de balises à un point d'accès, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- TagResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant montre comment ajouter des balises à un point d'accès à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3:region:111122223333:accesspoint/my-access-point/* \
--tags "Key=key1,Value=value1"
```

Réponse :

```
{
  "ResponseMetadata": {
      "RequestId": "EXAMPLE123456789",
      "HTTPStatusCode": 200,
      "HTTPHeaders": {
          "date": "Wed, 19 Jun 2025 10:30:00 GMT",
          "content-length": "0"
      },
      "RetryAttempts": 0
  }
}
```

Afficher les balises des points d'accès

Vous pouvez afficher ou répertorier les balises appliquées aux points d'accès. Pour en savoir plus sur les identifications, consultez Utilisation de balises avec des points d'accès S3 pour des compartiments à usage général.

Autorisations

Pour afficher les balises appliquées à un point d'accès, vous devez disposer des autorisations suivantes :

- `s3:ListTagsForResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de répertorier ou d'afficher les balises d'un point d'accès, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des informations requises Autorisations pour afficher ou répertorier les balises du point d'accès.

Étapes

Vous pouvez consulter les balises appliquées aux points d'accès à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour afficher les balises appliquées à un point d'accès à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (General Purpose Buckets).
3. Choisissez le nom du point d'accès.
4. Choisissez l'onglet Propriétés.
5. Accédez à la section Tags pour voir toutes les balises appliquées au point d'accès.
6. La section Tags affiche les tags définis par l'utilisateur par défaut. Vous pouvez sélectionner l'onglet balises AWS générées pour afficher les balises appliquées à votre point d'accès par les AWS services.

En utilisant le AWS SDKs

Cette section fournit un exemple de la façon d'afficher les balises appliquées à un point d'accès à l'aide du AWS SDKs.

SDK for Java 2.x

Cet exemple montre comment afficher les balises appliquées à un point d'accès à l'aide du AWS SDK for Java 2.x.

```
ListTagsForResourceRequest listTagsForResourceRequest = ListTagsForResourceRequest
```

```
.builder().resourceArn(arn:aws::s3:region:111122223333:accesspoint/my-access-point/
*)
                .accountId(111122223333).build();
awss3Control.listTagsForResource(listTagsForResourceRequest);
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST d'Amazon S3 pour l'affichage des balises appliquées à un point d'accès, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- ListTagsforResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant vous montre comment afficher les balises appliquées à un point d'accès. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3:region:444455556666:bucket/prefix--use1-az4--x-s3 \
```

Réponse : balises présentes :

```
{
  "Tags": [
      {
          "Key": "MyKey1",
          "Value": "MyValue1"
      },
      {
          "Key": "MyKey2",
          "Value": "MyValue2"
      },
```

```
        {
            "Key": "MyKey3",
            "Value": "MyValue3"
        }
    ]
}
```

Réponse : aucun tag n'est présent :

```
{
  "Tags": []
}
```

Supprimer un tag d'un point d'accès

Vous pouvez supprimer des balises des points d'accès Amazon S3. Une AWS balise est une paire clé-valeur qui contient des métadonnées sur les ressources, en l'occurrence les points d'accès. Pour en savoir plus sur les identifications, consultez Utilisation de balises avec des points d'accès S3 pour des compartiments à usage général.

> **Note**
>
> Si vous supprimez un tag et apprenez par la suite qu'il était utilisé pour suivre les coûts ou pour contrôler l'accès, vous pouvez le rajouter au point d'accès.

Autorisations

Pour supprimer un tag d'un point d'accès, vous devez disposer des autorisations suivantes :

- `s3:UntagResource`

Résolution des erreurs

Si vous rencontrez une erreur lorsque vous tentez de supprimer une étiquette d'un point d'accès, vous pouvez effectuer les opérations suivantes :

- Vérifiez que vous disposez des conditions requises Autorisations pour supprimer un tag d'un point d'accès.

Étapes

Vous pouvez supprimer des balises des points d'accès à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour supprimer des balises d'un point d'accès à l'aide de la console Amazon S3 :

1. Connectez-vous à la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Points (General Purpose Buckets).
3. Choisissez le nom du point d'accès.
4. Choisissez l'onglet Propriétés.
5. Accédez à la section Tags et cochez la case à côté du tag ou des tags que vous souhaitez supprimer.
6. Sélectionnez Delete (Supprimer).
7. La fenêtre contextuelle Supprimer les balises définies par l'utilisateur apparaît et vous demande de confirmer la suppression de la ou des balises que vous avez sélectionnées.
8. Choisissez Supprimer pour confirmer.

En utilisant le AWS SDKs

SDK for Java 2.x

Cet exemple montre comment supprimer des balises d'un point d'accès à l'aide du AWS SDK for Java 2.x. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

```
UntagResourceRequest tagResourceRequest = UntagResourceRequest.builder()
                .resourceArn(arn:aws::s3:region:111122223333:accesspoint/my-access-
point/*)
                .accountId(111122223333)
                .tagKeys(List.of("key1", "key2")).build();
awss3Control.untagResource(tagResourceRequest);
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la suppression de balises d'un point d'accès, consultez la section suivante du manuel Amazon Simple Storage Service API Reference :

- UnTagResource

En utilisant le AWS CLI

Pour installer la AWS CLI, reportez-vous à la section Installation de la AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

L'exemple de CLI suivant montre comment supprimer des balises d'un point d'accès à l'aide du AWS CLI. Pour utiliser la commande, remplacez les *user input placeholders* par vos propres informations.

Requête :

```
aws s3control untag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3:region:444455556666:access-point/my-access-point \
--tag-keys "tagkey1" "tagkey2"


  aws s3control untag-resource \
--account-id 111122223333 \
--resource-arn arn:aws::s3:region:444455556666:accesspointmy-access-point/* \
--tag-keys "key1" "key2"
```

Réponse :

```
{
  "ResponseMetadata": {
    "RequestId": "EXAMPLE123456789",
    "HTTPStatusCode": 204,
    "HTTPHeaders": {
        "date": "Wed, 19 Jun 2025 10:30:00 GMT",
        "content-length": "0"
    },
    "RetryAttempts": 0
```

```
  }
}
```

Gestion de l'accès avec les autorisations d'accès S3

Pour respecter le principe du moindre privilège, vous définissez un accès granulaire à vos données Amazon S3 en fonction des applications, des personas, des groupes ou des unités organisationnelles. Vous pouvez utiliser diverses approches pour mettre en place un accès granulaire aux données dans Amazon S3, en fonction de l'échelle et de la complexité des modèles d'accès.

L'approche la plus simple pour gérer l'accès à un small-to-medium certain nombre d'ensembles de données dans Amazon S3 par les principaux AWS Identity and Access Management (IAM) consiste à définir des politiques d'autorisation IAM et des politiques de compartiment S3. Cette stratégie fonctionne, à condition que les politiques nécessaires respectent les limites de taille des politiques de compartiment S3 (20 Ko) et des politiques IAM (5 Ko), ainsi que le nombre de principaux IAM autorisés par compte.

Avec l'augmentation du nombre de jeux de données et de cas d'utilisation, il se peut que vous ayez besoin de plus d'espace de politique. Une approche qui offre beaucoup plus d'espace pour les déclarations de politique consiste à utiliser les points d'accès S3 comme points de terminaison supplémentaires pour les compartiments S3, car chaque point d'accès peut avoir sa propre politique. Vous pouvez définir des modèles de contrôle d'accès très précis, car vous pouvez avoir des milliers de points d'accès Région AWS par compte, avec une politique d'une taille maximale de 20 Ko pour chaque point d'accès. Bien que les points d'accès S3 augmentent la quantité d'espace de politique disponible, ils nécessitent un mécanisme permettant aux clients de découvrir le point d'accès approprié pour le jeu de données approprié.

Une troisième approche consiste à implémenter un modèle d'agent de session IAM, dans lequel vous implémentez une logique de décision d'accès et générez dynamiquement des informations d'identification de session IAM à court terme pour chaque session d'accès. L'approche de l'agent de session IAM prend en charge les modèles d'autorisations arbitrairement dynamiques et s'adapte efficacement, mais vous devez élaborer la logique des modèles d'accès.

Au lieu d'utiliser ces approches, vous pouvez utiliser les autorisations d'accès S3 pour gérer l'accès à vos données Amazon S3. Les autorisations d'accès S3 fournissent un modèle simplifié pour définir les autorisations d'accès aux données dans Amazon S3 par préfixe, compartiment ou objet. En outre, vous pouvez utiliser les autorisations d'accès S3 pour accorder l'accès à la fois aux principaux IAM et directement aux utilisateurs ou groupes de votre annuaire d'entreprise.

Vous définissez généralement les autorisations d'accès aux données dans Amazon S3 en mappant les utilisateurs et les groupes aux jeux de données. Vous pouvez utiliser les autorisations d'accès S3 pour définir des mappages d'accès direct des préfixes S3 aux utilisateurs et aux rôles au sein des compartiments et des objets Amazon S3. Grâce au schéma d'accès simplifié des autorisations d'accès S3, vous pouvez accorder un accès en lecture seule, en écriture seule ou en lecture-écriture en fonction d'un préfixe S3 à la fois aux principaux IAM et directement aux utilisateurs ou groupes d'un annuaire d'entreprise. Grâce à ces fonctionnalités d'autorisations d'accès S3, les applications peuvent demander des données à Amazon S3 au nom de l'utilisateur authentifié actuel de l'application.

Lorsque vous intégrez les subventions d'accès S3 à la fonctionnalité de propagation d'identité sécurisée de AWS IAM Identity Center, vos applications peuvent envoyer des demandes Services AWS (y compris les subventions d'accès S3) directement au nom d'un utilisateur authentifié de l'annuaire d'entreprise. Vos applications n'ont plus besoin de commencer par mapper l'utilisateur à un principal IAM. En outre, étant donné que les identités des utilisateurs finaux sont propagées jusqu'à Amazon S3, l'audit permettant de vérifier quel utilisateur a accédé à quel objet S3 est simplifié. Il n'est plus nécessaire de reconstruire la relation entre les différents utilisateurs et les sessions IAM. Lorsque vous utilisez les autorisations d'accès S3 avec la propagation d'identité approuvée d'IAM Identity Center, chaque événement de données AWS CloudTrail pour Amazon S3 contient une référence directe à l'utilisateur final pour le compte duquel les données ont été consultées.

La propagation fiable des identités est une AWS IAM Identity Center fonctionnalité que les administrateurs de Connected Services AWS peuvent utiliser pour accorder et auditer l'accès aux données de service. L'accès à ces données est basé sur les attributs de l'utilisateur tels que les associations de groupes. La mise en place d'une propagation d'identité sécurisée nécessite une collaboration entre les administrateurs de Connected Services AWS et les administrateurs d'IAM Identity Center. Pour plus d'informations, consultez la section Conditions préalables et considérations.

Pour plus d'informations sur les autorisations d'accès S3, consultez les rubriques suivantes.

Rubriques

- Concepts des autorisations d'accès S3
- Autorisations d'accès S3 et identités d'annuaire d'entreprise
- Bien démarrer avec les autorisations d'accès S3
- Utilisation des instances d'autorisations d'accès S3
- Utilisation des emplacements d'autorisations d'accès S3

- Octroi d'autorisations avec les autorisations d'accès S3
- Obtention de données S3 à l'aide d'autorisations d'accès
- Accès intercompte aux autorisations d'accès S3
- Gestion des balises pour les subventions d'accès S3
- Limitations des autorisations d'accès S3
- Intégrations des autorisations d'accès S3

Concepts des autorisations d'accès S3

Flux de travail des autorisations d'accès S3

Le flux de travail des autorisations d'accès S3 est le suivant :

1. Créez une instance d'autorisations d'accès S3. Consultez Utilisation des instances d'autorisations d'accès S3.
2. Dans votre instance S3 Access Grants, enregistrez des emplacements dans vos données Amazon S3 et associez ces emplacements à des rôles AWS Identity and Access Management (IAM). Consultez Enregistrement d'un emplacement.
3. Créez des autorisations pour les bénéficiaires, qui leur permettent d'accéder à vos ressources S3. Consultez Octroi d'autorisations avec les autorisations d'accès S3.
4. Le bénéficiaire demande des informations d'identification temporaires aux autorisations d'accès S3. Consultez Demande d'un accès aux données Amazon S3 via les autorisations d'accès S3.
5. Le bénéficiaire accède aux données S3 à l'aide de ces informations d'identification temporaires. Consultez Accès aux données S3 à l'aide des informations d'identification fournies par les autorisations d'accès S3.

Pour de plus amples informations, veuillez consulter Bien démarrer avec les autorisations d'accès S3.

Instances d'autorisations d'accès S3

> Une instance d'autorisations d'accès S3 est un conteneur logique pour les autorisations individuelles. Lorsque vous créez une instance d'autorisations d'accès S3, vous devez spécifier une Région AWS. Chacun Région AWS d'entre vous Compte AWS peut avoir une instance S3 Access Grants. Pour de plus amples informations, veuillez consulter Utilisation des instances d'autorisations d'accès S3.

Si vous souhaitez utiliser S3 Access Grants pour accorder l'accès aux identités d'utilisateurs et de groupes à partir de votre annuaire d'entreprise, vous devez également associer votre instance S3 Access Grants à une AWS IAM Identity Center instance. Pour de plus amples informations, veuillez consulter Autorisations d'accès S3 et identités d'annuaire d'entreprise.

Une instance d'autorisations d'accès S3 qui vient d'être créée est vide. Vous devez enregistrer un emplacement dans l'instance, qui peut être le chemin par défaut S3 (`s3://`), un compartiment ou un préfixe au sein d'un compartiment. Après avoir enregistré au moins un emplacement, vous pouvez créer des autorisations d'accès qui donnent accès aux données de cet emplacement.

Emplacements

Un emplacement S3 Access Grants associe des compartiments ou des préfixes à un rôle AWS Identity and Access Management (IAM). Les autorisations d'accès S3 endosseront ce rôle IAM pour fournir des informations d'identification temporaires au bénéficiaire qui accédera à cet emplacement particulier. Vous devez d'abord enregistrer au moins un emplacement auprès de votre instance d'autorisations d'accès S3 avant de pouvoir créer des autorisations d'accès.

Nous vous recommandons d'enregistrer l'emplacement par défaut (`s3://`) et de le mapper à un rôle IAM. L'emplacement sur le chemin S3 par défaut (`s3://`) couvre l'accès à tous vos compartiments S3 Région AWS de votre compte. Lorsque vous créez une autorisation d'accès, vous pouvez restreindre la portée de cette autorisation à un compartiment, à un préfixe ou à un objet situé à l'emplacement par défaut.

Les cas d'utilisation plus complexes liés à la gestion des accès peuvent vous obliger à enregistrer un autre emplacement que l'emplacement par défaut. Voici quelques exemples de tels cas d'utilisation :

- Supposons qu'*`amzn-s3-demo-bucket`* soit un emplacement enregistré dans votre instance d'autorisations d'accès S3 et qu'un rôle IAM lui soit associé, mais que ce rôle IAM se voit refuser l'accès à un préfixe particulier dans le compartiment. Dans ce cas, vous pouvez enregistrer le préfixe auquel le rôle IAM n'a pas accès en tant qu'emplacement distinct et associer cet emplacement à un autre rôle IAM disposant de l'accès nécessaire.
- Supposons que vous souhaitiez créer des autorisations qui limitent l'accès aux utilisateurs au sein d'un point de terminaison de cloud privé virtuel (VPC). Dans ce cas, vous pouvez enregistrer un emplacement pour un compartiment dans lequel le rôle IAM restreint l'accès à ce point de terminaison du VPC. Ultérieurement, lorsqu'un bénéficiaire demandera des informations d'identification aux autorisations d'accès S3, les autorisations d'accès S3 endosseront le rôle IAM de l'emplacement pour fournir des informations d'identification temporaires. Ces informations d'identification refuseront l'accès au compartiment spécifique,

sauf si l'appelant se trouve dans le point de terminaison du VPC. Cette autorisation de refus sera appliquée en plus de l'autorisation READ, WRITE ou READWRITE habituellement spécifiée dans l'autorisation d'accès.

Si votre cas d'utilisation vous oblige à enregistrer plusieurs emplacements dans votre instance d'autorisations d'accès S3, vous pouvez enregistrer l'un des emplacements suivants :

- Emplacement par défaut (`s3://`)
- Un compartiment (par exemple, *`amzn-s3-demo-bucket`*) ou plusieurs compartiments
- Un compartiment et un préfixe (par exemple, *`amzn-s3-demo-bucket`*`/prefix*`) ou plusieurs préfixes

Pour connaître le nombre maximal d'emplacements que vous pouvez enregistrer dans votre instance d'autorisations d'accès S3, consultez Limitations des autorisations d'accès S3. Pour plus d'informations sur l'enregistrement d'un emplacement d'autorisations d'accès S3, consultez Enregistrement d'un emplacement.

Une fois que vous avez enregistré le premier emplacement dans votre instance d'autorisations d'accès S3, celle-ci ne dispose toujours d'aucune autorisation d'accès individuelle. Aucun accès n'a donc encore été accordé à aucune de vos données S3. Vous pouvez désormais créer des autorisations d'accès pour accorder un accès. Pour plus d'informations sur la création d'autorisations d'accès, consultez Octroi d'autorisations avec les autorisations d'accès S3.

Octrois

Une autorisation individuelle dans une instance d'autorisations d'accès S3 permet à une identité spécifique, à savoir un principal IAM ou un utilisateur/groupe dans un annuaire d'entreprise, d'obtenir l'accès à un emplacement qui est enregistré dans votre instance d'autorisations d'accès S3.

Lorsque vous créez une autorisation, vous n'êtes pas obligé d'accorder l'accès à l'ensemble de l'emplacement enregistré. Vous pouvez limiter l'étendue de l'accès de l'autorisation au sein d'un emplacement. Si l'emplacement enregistré est le chemin S3 par défaut (`s3://`), vous devez limiter la portée de l'autorisation à un compartiment, à un préfixe dans un compartiment ou à un objet spécifique. Si l'emplacement enregistré de l'autorisation est un compartiment ou un préfixe, vous pouvez donner accès à l'intégralité du compartiment ou du préfixe, ou vous pouvez aussi restreindre la portée de l'autorisation à un préfixe, un sous-préfixe ou un objet.

Dans l'autorisation, vous définissez également son niveau d'accès sur READ, WRITE ou READWRITE. Supposons que vous disposiez d'une autorisation qui donne au groupe de

l'annuaire d'entreprise `01234567-89ab-cdef-0123-456789abcdef` l'accès en lecture au compartiment `s3://amzn-s3-demo-bucket/projects/items/*`. Les utilisateurs de ce groupe peuvent avoir un accès READ à chaque objet dont le nom de clé d'objet commence par le préfixe `projects/items/` dans le compartiment nommé *amzn-s3-demo-bucket*.

Pour le nombre maximum d'autorisations d'accès que vous pouvez créer dans votre instance d'autorisations d'accès S3, consultez Limitations des autorisations d'accès S3. Pour plus d'informations sur la création d'autorisations d'accès, consultez Création d'octrois.

Informations d'identification temporaires des autorisations d'accès S3

Une fois que vous avez créé une autorisation, une application autorisée qui utilise l'identité spécifiée dans l'autorisation peut demander des informations d'just-in-time accès. Pour ce faire, l'application appelle l'opération d'API GetDataAccessS3. Les bénéficiaires peuvent utiliser cette opération d'API pour demander l'accès aux données S3 que vous avez partagées avec eux.

L'instance d'autorisations d'accès S3 évalue la demande `GetDataAccess` par rapport aux autorisations dont elle dispose. S'il existe une autorisation correspondante pour le demandeur, les autorisations d'accès S3 endossent le rôle IAM associé à l'emplacement de cette autorisation. Les autorisations d'accès S3 délimitent ensuite les autorisations de la session IAM précisément au compartiment, préfixe ou objet S3 spécifié par l'étendue de l'octroi.

Le délai d'expiration des informations d'identification d'accès temporaire est défini par défaut sur 1 heure, mais vous pouvez le définir sur une valeur quelconque comprise entre 15 minutes et 12 heures. Consultez la durée maximale de session dans la référence de AssumeRolel'API.

Comment ça marche

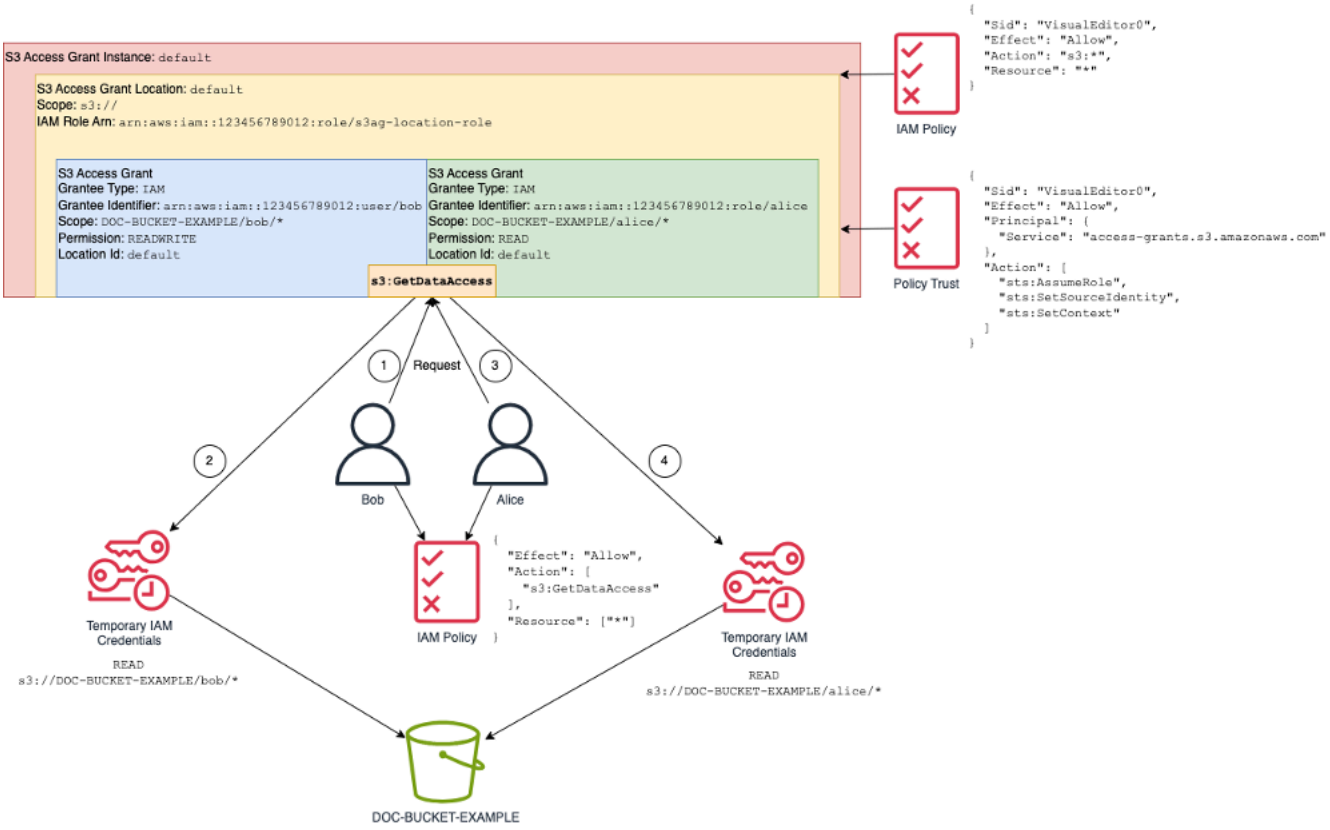
Dans le schéma suivant, un emplacement Amazon S3 par défaut avec la ^portée `s3://` est enregistré avec le rôle IAM `s3ag-location-role`. Ce rôle IAM est autorisé à effectuer des actions Amazon S3 dans le compte lorsque ses informations d'identification sont obtenues via les autorisations d'accès S3.

Au sein de cet emplacement, deux autorisations d'accès individuelles sont créées pour deux utilisateurs IAM. L'utilisateur IAM Bob se voit octroyer l'accès `READ` et l'accès `WRITE` sur le préfixe `bob/` dans le compartiment `DOC-BUCKET-EXAMPLE`. Un autre rôle IAM, Alice, se voit octroyer uniquement l'accès `READ` sur le préfixe `alice/` dans le compartiment `DOC-BUCKET-EXAMPLE`. Un octroi, coloré en bleu, est défini pour permettre à Bob d'accéder au préfixe `bob/` dans le

compartiment DOC-BUCKET-EXAMPLE. Un octroi, coloré en vert, est défini pour permettre à Alice d'accéder au préfixe alice/ dans le compartiment DOC-BUCKET-EXAMPLE.

Lorsqu'il est temps pour Bob d'accéder aux READ données, le rôle IAM associé à l'emplacement dans lequel se trouve sa subvention appelle l'opération d'GetDataAccessAPI S3 Access Grants. Si Bob essaie de lire (READ) un préfixe ou un objet S3 quelconque commençant par s3://DOC-BUCKET-EXAMPLE/bob/*, la demande GetDataAccess renvoie un ensemble d'informations d'identification de session IAM temporaires avec l'autorisation à s3://DOC-BUCKET-EXAMPLE/bob/*. De même, Bob peut écrire (WRITE) sur n'importe quel préfixe ou objet S3 commençant par s3://DOC-BUCKET-EXAMPLE/bob/*, car l'octroi le permet également.

De même, Alice peut lire (READ) tout ce qui commence par s3://DOC-BUCKET-EXAMPLE/alice/. Toutefois, si elle essaie d'écrire (WRITE) sur un compartiment, un préfixe ou un objet quelconque dans s3://, elle recevra une erreur Accès refusé (403 Forbidden), car aucun octroi ne lui donne l'accès WRITE sur aucune donnée. En outre, si Alice demande un niveau d'accès quelconque (READ ou WRITE) à des données situées en dehors de s3://DOC-BUCKET-EXAMPLE/alice/, elle recevra à nouveau une erreur Accès refusé.



Ce modèle s'adapte à un nombre élevé d'utilisateurs et de compartiments, et simplifie la gestion de ces autorisations. Au lieu de modifier des politiques de compartiment S3 potentiellement

volumineuses chaque fois que vous souhaitez ajouter ou supprimer une relation individuelle d'accès par préfixe utilisateur, vous pouvez ajouter et supprimer des octrois discrets et individuels.

Autorisations d'accès S3 et identités d'annuaire d'entreprise

Vous pouvez utiliser les subventions d'accès Amazon S3 pour accorder l'accès aux principaux AWS Identity and Access Management (utilisateurs ou rôles) (IAM), à la fois dans le même environnement Compte AWS et dans d'autres. Toutefois, dans de nombreux cas, l'entité accédant aux données est un utilisateur final issu de votre annuaire d'entreprise. Au lieu d'accorder l'accès aux principaux IAM, vous pouvez utiliser les autorisations d'accès S3 pour accorder l'accès directement aux utilisateurs et aux groupes de votre entreprise. Avec les autorisations d'accès S3, vous n'avez plus besoin de mapper vos identités d'entreprise à des principaux IAM intermédiaires pour accéder à vos données S3 via vos applications d'entreprise.

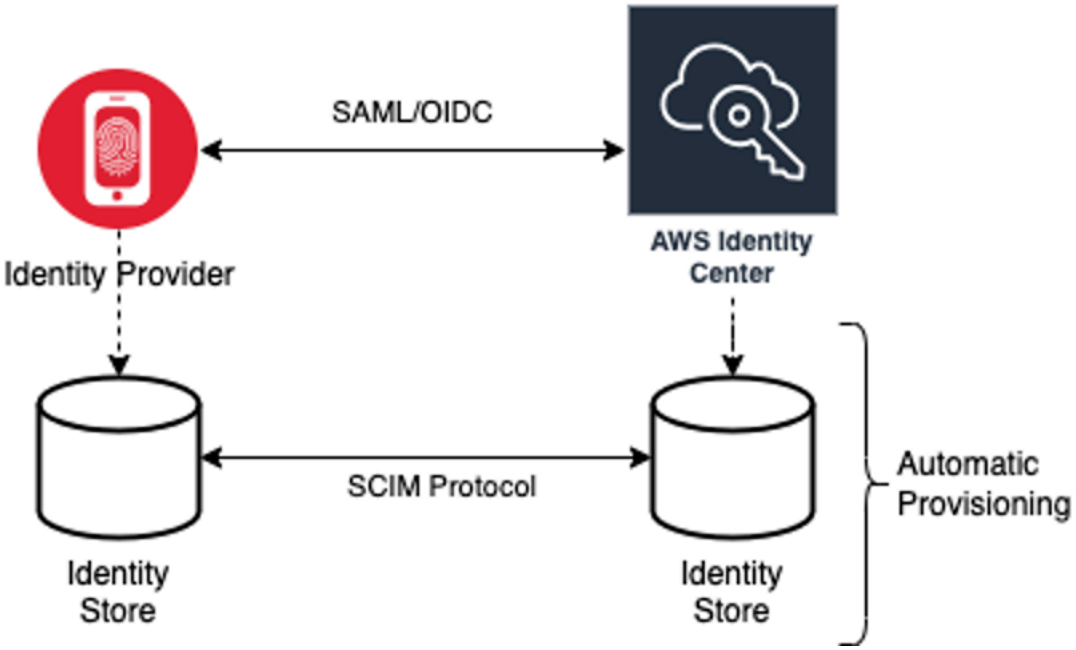
Cette nouvelle fonctionnalité (prise en charge de l'utilisation des identités des utilisateurs finaux pour accéder aux données) est fournie en associant votre instance S3 Access Grants à une instance. AWS IAM Identity Center IAM Identity Center prend en charge les fournisseurs d'identité basés sur des normes et constitue la plaque tournante AWS pour tous les services ou fonctionnalités, y compris les subventions d'accès S3, qui prennent en charge les identités des utilisateurs finaux. IAM Identity Center fournit un support d'authentification pour les identités d'entreprise via sa fonctionnalité de propagation d'identité approuvée. Pour plus d'informations, consultez Propagation d'identité approuvée entre applications.

Pour commencer à prendre en charge l'identité du personnel dans les autorisations d'accès S3, vous devez configurer au préalable le provisionnement des identités entre votre fournisseur d'identité d'entreprise et IAM Identity Center dans IAM Identity Center. IAM Identity Center prend en charge les fournisseurs d'identité d'entreprise tels que Okta, Microsoft Entra ID (anciennement Azure Active Directory) ou tout autre fournisseur d'identité (IdP) externe prenant en charge le protocole de mise en service du système de gestion des identités inter-domaines (SCIM). Lorsque vous connectez IAM Identity Center à votre fournisseur d'identité et que vous activez le provisionnement automatique, les utilisateurs et les groupes de votre IdP sont synchronisés dans le magasin d'identités d'IAM Identity Center. Après cette étape, IAM Identity Center dispose de sa propre vision de vos utilisateurs et de vos groupes, de sorte que vous pouvez y faire référence en utilisant d'autres Services AWS fonctionnalités, telles que S3 Access Grants. Pour plus d'informations sur la configuration du provisionnement automatique d'IAM Identity Center, consultez Provisionnement automatique dans le Guide de l'utilisateur AWS IAM Identity Center .

IAM Identity Center est intégré AWS Organizations afin que vous puissiez gérer de manière centralisée les autorisations sur plusieurs comptes Comptes AWS sans configurer manuellement chacun de vos comptes. Dans une organisation standard, votre administrateur d'identité configure une seule instance IAM Identity Center pour l'organisation tout entière, en tant que point unique de synchronisation des identités. Cette instance IAM Identity Center s'exécute généralement dans une instance dédiée Compte AWS de votre organisation. Dans cette configuration courante, vous pouvez faire référence aux identités des utilisateurs et des groupes dans S3 Access Grants depuis n'importe quel Compte AWS membre de l'organisation.

Toutefois, si votre AWS Organizations administrateur n'a pas encore configuré d'instance centrale d'IAM Identity Center, vous pouvez en créer une locale sur le même compte que votre instance S3 Access Grants. Une telle configuration est plus courante pour les cas proof-of-concept d'utilisation liés au développement local. Dans tous les cas, l'instance IAM Identity Center doit être Région AWS identique à l'instance S3 Access Grants à laquelle elle sera associée.

Dans le schéma suivant d'une configuration IAM Identity Center avec un IdP externe, le fournisseur d'identité est configuré avec SCIM pour synchroniser le magasin d'identités de l'IdP avec le magasin d'identités dans IAM Identity Center.



Pour utiliser vos identités d'annuaire d'entreprise avec les autorisations d'accès S3, procédez comme suit :

- Configurez le provisionnement automatique dans IAM Identity Center pour synchroniser les informations relatives aux utilisateurs et aux groupes entre votre fournisseur d'identité et IAM Identity Center.
- Configurez votre source d'identité externe dans IAM Identity Center en tant qu'émetteur de jetons approuvé. Pour plus d'informations, consultez Propagation d'identité approuvée entre applications dans le Guide de l'utilisateur AWS IAM Identity Center .
- Associez votre instance d'autorisations d'accès S3 à votre instance IAM Identity Center. Vous pouvez le faire lorsque vous créez votre instance d'autorisations d'accès S3. Si vous avez déjà créé votre instance d'autorisations d'accès S3, consultez Association ou dissociation de votre instance IAM Identity Center.

Accès des identités d'annuaire aux données S3

Supposons que vous ayez des utilisateurs d'annuaire d'entreprise qui ont besoin d'accéder à vos données S3 via une application d'entreprise, par exemple, une visionneuse de documents intégrée à votre fournisseur d'identité externe (par exemple, Okta) pour authentifier les utilisateurs. L'authentification de l'utilisateur dans ces applications se fait généralement par le biais de redirections dans le navigateur Web de l'utilisateur. Comme les utilisateurs figurant dans l'annuaire ne sont pas des principaux IAM, votre application a besoin d'informations d'identification IAM pour appeler l'opération d'API `GetDataAccess` des autorisations d'accès S3 afin d'obtenir des informations d'identification d'accès aux données S3 au nom des utilisateurs. Contrairement aux utilisateurs et aux rôles IAM qui obtiennent eux-mêmes des informations d'identification, votre application a besoin d'un moyen de représenter un utilisateur d'annuaire non mappé à un rôle IAM, afin que l'utilisateur puisse accéder aux données via les autorisations d'accès S3.

Cette transition, d'un utilisateur d'annuaire authentifié à un appelant IAM capable d'adresser des demandes aux autorisations d'accès S3 au nom de l'utilisateur d'annuaire, est effectuée par l'application via la fonctionnalité d'émetteur de jetons approuvé d'IAM Identity Center. Après avoir authentifié l'utilisateur d'annuaire, l'application dispose d'un jeton d'identité provenant du fournisseur d'identité (par exemple, Okta) qui représente l'utilisateur d'annuaire selon Okta. La configuration de l'émetteur de jetons approuvé dans IAM Identity Center permet à l'application d'échanger ce jeton Okta (le locataire Okta est configuré comme « émetteur approuvé ») contre un autre jeton d'identité issu d'IAM Identity Center qui représentera de manière sécurisée l'utilisateur d'annuaire au sein des Services AWS. L'application de données endosse alors un rôle IAM, fournissant le jeton de l'utilisateur d'annuaire provenant d'IAM Identity Center comme contexte supplémentaire. L'application peut utiliser la session IAM qui en résulte pour appeler des autorisations d'accès S3.

Le jeton représente à la fois l'identité de l'application (le principal IAM lui-même) et l'identité de l'utilisateur d'annuaire.

L'étape principale de cette transition est l'échange de jetons. L'application effectue cet échange de jetons en appelant l'opération d'API `CreateTokenWithIAM` dans IAM Identity Center. Bien entendu, il s'agit également d'un appel d' AWS API qui nécessite la signature d'un directeur IAM. Le principal IAM qui effectue cette demande est généralement un rôle IAM associé à l'application. Par exemple, si l'application s'exécute sur Amazon EC2, la `CreateTokenWithIAM` demande est généralement exécutée par le rôle IAM associé à l' EC2 instance sur laquelle l'application s'exécute. Le résultat d'un `CreateTokenWithIAM` appel réussi est un nouveau jeton d'identité, qui sera reconnu à l'intérieur Services AWS.

L'étape suivante, avant que l'application puisse appeler `GetDataAccess` au nom de l'utilisateur d'annuaire, consiste pour l'application à obtenir une session IAM incluant l'identité de l'utilisateur d'annuaire. Pour ce faire, l'application utilise une `AssumeRole` demande AWS Security Token Service (AWS STS) qui inclut également le jeton IAM Identity Center pour l'utilisateur de l'annuaire en tant que contexte d'identité supplémentaire. Ce contexte supplémentaire permet à IAM Identity Center de propager l'identité de l'utilisateur d'annuaire à l'étape suivante. Le rôle IAM endossé par l'application est celui qui nécessitera des autorisations IAM pour appeler l'opération `GetDataAccess`.

Après avoir endossé le rôle IAM du porteur d'identité avec le jeton IAM Identity Center pour l'utilisateur d'annuaire comme contexte supplémentaire, l'application dispose désormais de tout ce dont elle a besoin pour adresser une demande signée à `GetDataAccess` au nom de l'utilisateur d'annuaire authentifié.

La propagation des jetons se base sur les étapes suivantes :

Création d'une application IAM Identity Center

Commencez par créer une nouvelle application dans IAM Identity Center. Cette application utilisera un modèle permettant à IAM Identity Center d'identifier le type de paramètres d'application que vous pouvez utiliser. La commande pour créer l'application nécessite que vous fournissiez l'Amazon Resource Name (ARN) de l'instance IAM Identity Center, un nom d'application et l'ARN du fournisseur d'application. Le fournisseur d'applications est le SAML ou le fournisseur OAuth d'applications que l'application utilisera pour passer des appels à IAM Identity Center.

Pour utiliser l'exemple de commande suivant, remplacez les *`user input placeholders`* par vos propres informations :

```
aws sso-admin create-application \
 --instance-arn "arn:aws:sso:::instance/ssoins-ssoins-1234567890abcdef" \
 --application-provider-arn "arn:aws:sso::aws:applicationProvider/custom" \
 --name MyDataApplication
```

Réponse :

```
{
   "ApplicationArn": "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
}
```

Création d'un émetteur de jetons approuvé

Maintenant que vous disposez d'une application IAM Identity Center, l'étape suivante consiste à configurer un émetteur de jetons approuvé qui permettra d'échanger vos valeurs `IdToken` de votre fournisseur d'identité contre des jetons IAM Identity Center. Dans cette étape, vous devez fournir les éléments suivants :

- URL de l'émetteur du fournisseur d'identité
- Nom de l'émetteur de jetons approuvé
- Chemin d'attribut de demande
- Chemin d'attribut de magasin d'identités
- Option de récupération de l'ensemble de clés web JSON (JWKS)

Le chemin d'attribut de demande est l'attribut du fournisseur d'identité qui sera utilisé pour la mappage à l'attribut de magasin d'identités. Normalement, le chemin d'attribut de demande est l'adresse e-mail de l'utilisateur, mais vous pouvez utiliser d'autres attributs pour effectuer le mappage.

Créez un fichier appelé `oidc-configuration.json` avec les informations suivantes. Pour utiliser ce fichier, remplacez les *`user input placeholders`* par vos propres informations.

```
{
  "OidcJwtConfiguration":
     {
      "IssuerUrl": "https://login.microsoftonline.com/a1b2c3d4-abcd-1234-b7d5-
b154440ac123/v2.0",
      "ClaimAttributePath": "preferred_username",
```

```
      "IdentityStoreAttributePath": "userName",
      "JwksRetrievalOption": "OPEN_ID_DISCOVERY"
     }
}
```

Pour créer l'émetteur de jetons approuvé, exécutez la commande suivante. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws sso-admin create-trusted-token-issuer \
  --instance-arn "arn:aws:sso:::instance/ssoins-1234567890abcdef" \
  --name MyEntraIDTrustedIssuer \
  --trusted-token-issuer-type OIDC_JWT \
  --trusted-token-issuer-configuration file://./oidc-configuration.json
```

Réponse

```
{
  "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234"
}
```

Connexion de l'application IAM Identity Center à l'émetteur de jetons approuvé

L'émetteur de jetons approuvé a besoin de quelques paramètres de configuration supplémentaires pour fonctionner. Définissez l'audience à laquelle l'émetteur de jetons approuvé fera confiance. L'audience est la valeur figurant dans `IdToken` qui est identifiée par la clé et qui se trouve dans les paramètres du fournisseur d'identité. Par exemple :

```
1234973b-abcd-1234-abcd-345c5a9c1234
```

Créez un fichier nommé `grant.json` qui contient le contenu suivant. Pour utiliser ce fichier, modifiez l'audience afin qu'elle corresponde aux paramètres de votre fournisseur d'identité et fournissez l'ARN de l'émetteur de jetons approuvé renvoyé par la commande précédente.

```
{
   "JwtBearer":
     {
       "AuthorizedTokenIssuers":
         [
           {
```

```
            "TrustedTokenIssuerArn": "arn:aws:sso::123456789012:trustedTokenIssuer/
ssoins-1234567890abcdef/tti-43b4a822-1234-1234-1234-a1b2c3d41234",
              "AuthorizedAudiences":
                [
                  "1234973b-abcd-1234-abcd-345c5a9c1234"
                ]
            }
          ]
      }
 }
```

Exécutez l'exemple de commande suivant. Pour utiliser cette commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws sso-admin put-application-grant \
  --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
  --grant-type "urn:ietf:params:oauth:grant-type:jwt-bearer" \
  --grant file://./grant.json \
```

Cette commande définit les paramètres de configuration de l'émetteur de jetons approuvé pour qu'il fasse confiance à l'audience définie dans le fichier `grant.json` et relie cette audience à l'application créée à la première étape pour échanger des jetons du type `jwt-bearer`. La chaîne `urn:ietf:params:oauth:grant-type:jwt-bearer` n'est pas une chaîne arbitraire. Il s'agit d'un espace de noms enregistré dans les profils d'assertion OAuth JSON Web Token (JWT). Vous trouverez plus d'informations sur cet espace de noms dans la RFC 7523.

Ensuite, utilisez la commande suivante pour définir les portées que l'émetteur de jetons approuvé inclura lors de l'échange de valeurs `IdToken` à partir de votre fournisseur d'identité. Pour les autorisations d'accès S3, la valeur du paramètre `--scope` est `s3:access_grants:read_write`.

```
aws sso-admin put-application-access-scope \
  --application-arn "arn:aws:sso::111122223333:application/ssoins-
ssoins-111122223333abcdef/apl-abcd1234a1b2c3d" \
  --scope "s3:access_grants:read_write"
```

La dernière étape consiste à attacher une politique de ressources à l'application IAM Identity Center. Cette politique permettra au rôle IAM de votre application d'adresser des demandes à l'opération d'API `sso-oauth:CreateTokenWithIAM` et de recevoir les valeurs `IdToken` d'IAM Identity Center.

Créez un fichier nommé `authentication-method.json` qui contient le contenu suivant. Remplacez *123456789012* par votre ID de compte.

```
{
   "Iam":
       {
         "ActorPolicy":
             {
                "Version": "2012-10-17",
                    "Statement":
                    [
                        {
                           "Effect": "Allow",
                            "Principal":
                            {
                              "AWS": "arn:aws:iam::123456789012:role/webapp"
                            },
                           "Action": "sso-oauth:CreateTokenWithIAM",
                            "Resource": "*"
                        }
                    ]
                }
            }
        }
```

Pour attacher la politique à l'application IAM Identity Center, exécutez la commande suivante :

```
aws sso-admin put-application-authentication-method \
   --application-arn "arn:aws:sso::123456789012:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d" \
   --authentication-method-type IAM \
   --authentication-method file://./authentication-method.json
```

Ceci complète les paramètres de configuration pour l'utilisation des autorisations d'accès S3 avec les utilisateurs d'annuaire via une application Web. Vous pouvez tester cette configuration directement dans l'application ou vous pouvez appeler l'opération d'API `CreateTokenWithIAM` en utilisant la commande suivante à partir d'un rôle IAM autorisé dans la politique d'application IAM Identity Center :

```
aws sso-oidc create-token-with-iam \
   --client-id "arn:aws:sso::123456789012:application/ssoins-ssoins-1234567890abcdef/
apl-abcd1234a1b2c3d"  \
```

```
   --grant-type urn:ietf:params:oauth:grant-type:jwt-bearer \
   --assertion IdToken
```

La réponse sera similaire à ceci :

```
{
    "accessToken": "<suppressed long string to reduce space>",
    "tokenType": "Bearer",
    "expiresIn": 3600,
    "refreshToken": "<suppressed long string to reduce space>",
    "idToken": "<suppressed long string to reduce space>",
    "issuedTokenType": "urn:ietf:params:oauth:token-type:refresh_token",
    "scope": [
      "sts:identity_context",
      "s3:access_grants:read_write",
      "openid",
      "aws"
    ]
}
```

Si vous décodez la valeur `IdToken` codée en base64, vous pouvez voir les paires clé-valeur au format JSON. La clé `sts:identity_context` contient la valeur que votre application doit envoyer dans la demande `sts:AssumeRole` pour inclure les informations d'identité de l'utilisateur d'annuaire. Voici un exemple de valeur `IdToken` décodée :

```
{
    "aws:identity_store_id": "d-996773e796",
    "sts:identity_context": "AQoJb3JpZ2luX2VjEOTtl;<SUPRESSED>",
    "sub": "83d43802-00b1-7054-db02-f1d683aacba5",
    "aws:instance_account": "123456789012",
    "iss": "https://identitycenter.amazonaws.com/ssoins-1234567890abcdef",
    "sts:audit_context": "AQoJb3JpZ2luX2VjEOT<SUPRESSED>==",
    "aws:identity_store_arn": "arn:aws:identitystore::232642235904:identitystore/
d-996773e796",
    "aud": "abcd12344U0gi7n4Yyp0-WV1LWNlbnRyYWwtMQ",
    "aws:instance_arn": "arn:aws:sso:::instance/ssoins-6987d7fb04cf7a51",
    "aws:credential_id": "EXAMPLEHI5glPh40y9TpApJn8...",
    "act": {
       "sub": "arn:aws:sso::232642235904:trustedTokenIssuer/
ssoins-6987d7fb04cf7a51/43b4a822-1020-7053-3631-cb2d3e28d10e"
    },
    "auth_time": "2023-11-01T20:24:28Z",
```

```
    "exp": 1698873868,
    "iat": 1698870268
}
```

Vous pouvez obtenir la valeur à partir de `sts:identity_context` et transmettre ces informations dans un appel `sts:AssumeRole`. Vous trouverez ci-dessous un exemple CLI de la syntaxe. Le rôle à endosser est un rôle temporaire avec des autorisations pour invoquer `s3:GetDataAccess`.

```
aws sts assume-role \
   --role-arn "arn:aws:iam::123456789012:role/temp-role" \
   --role-session-name "TempDirectoryUserRole" \
   --provided-contexts ProviderArn="arn:aws:iam::aws:contextProvider/
IdentityCenter",ContextAssertion="value from sts:identity_context"
```

Vous pouvez désormais utiliser les informations d'identification reçues à partir de cet appel pour invoquer l'opération d'API `s3:GetDataAccess` et recevoir les informations d'identification finales avec accès à vos ressources S3.

Bien démarrer avec les autorisations d'accès S3

Les autorisations d'accès Amazon S3 sont une fonctionnalité Amazon S3 qui fournit une solution de contrôle d'accès évolutive pour vos données S3. Les autorisations d'accès S3 sont un fournisseur d'informations d'identification S3, ce qui signifie que vous enregistrez avec eux votre liste d'octrois et le niveau d'accès. Par la suite, lorsque des utilisateurs ou des clients ont besoin d'accéder à vos données S3, ils demandent d'abord leurs informations d'identification aux autorisations d'accès S3. S'il existe un octroi correspondant qui autorise l'accès, les autorisations d'accès S3 proposent des informations d'identification d'accès temporaires de moindre privilège. Les utilisateurs ou les clients peuvent alors utiliser les informations d'identification proposées par les autorisations d'accès S3 pour accéder à vos données S3. Dans cette optique, si vos exigences en matière de données S3 nécessitent une configuration d'autorisations complexe ou importante, vous pouvez utiliser les autorisations d'accès S3 pour mettre à l'échelle les autorisations de données S3 pour les utilisateurs, les groupes, les rôles et les applications.

Dans la plupart des cas d'utilisation, vous pouvez gérer le contrôle d'accès à vos données S3 en utilisant AWS Identity and Access Management (IAM) avec des politiques de compartiment ou des politiques basées sur l'identité IAM.

Toutefois, si vous avez des exigences complexes en matière de contrôle d'accès S3, telles que les suivantes, vous pourriez tirer un grand avantage de l'utilisation d'autorisations d'accès S3 :

- Vous êtes confronté à la limite de taille de 20 Ko fixée par la politique de compartiment.
- Vous accordez aux identités humaines, telles que les utilisateurs et groupes Microsoft Entra ID (anciennement Azure Active Directory), Okta ou Ping, l'accès aux données S3 pour l'analytique et le big data.
- Vous devez fournir un accès intercompte sans mettre à jour fréquemment les politiques IAM.
- Vos données sont non structurées et de niveau objet au lieu d'être structurées, dans un format de lignes et de colonnes.

Le flux de travail des autorisations d'accès S3 est le suivant :

Étapes	Description
1	Création d'une instance d'autorisations d'accès S3 Pour commencer, lancez une instance d'autorisations d'accès S3 qui contiendra vos autorisations d'accès individuelles.
2	Enregistrement d'un emplacement Ensuite, enregistrez un emplacement de données S3 (tel que l'emplacement par défaut, `s3://`), puis spécifiez un rôle IAM par défaut que les autorisations d'accès S3 endossent lorsqu'il s fournissent l'accès à l'emplacement de données S3. Vous pouvez également ajouter des emplacements personnalisés à des compartiments ou à des préfixes spécifiques, et les mapper à des rôles IAM personnalisés.
3	Création d'octrois Créez des octrois d'autorisation individuels. Spécifiez dans ces octrois d'autorisation l'emplacement S3 enregistré, la portée de l'accès aux données au sein de cet emplacement, l'identit é du bénéficiaire et son niveau d'accès (`READ`, `WRITE` ou `READWRITE`).
4	Demande d'accès aux données S3

Étapes	Description
	Lorsque les utilisateurs, les applications et les utilisateurs Services AWS souhaitent accéder aux données S3, ils font d'abord une demande d'accès. Les autorisations d'accès S3 déterminent si la demande doit être autorisée. S'il existe une autorisation correspondante qui autorise l'accès, les autorisations d'accès S3 utilisent le rôle IAM de l'emplacement enregistré associé à cette autorisation pour proposer des informations d'identification temporaires en retour au demandeur.
5	Accédez aux données S3 Les applications utilisent les informations d'identification temporaires proposées par les autorisations d'accès S3 pour accéder aux données S3.

Utilisation des instances d'autorisations d'accès S3

Pour commencer à utiliser les autorisations d'accès Amazon S3, vous devez d'abord créer une instance d'autorisations d'accès S3. Vous ne pouvez créer qu'une seule instance S3 Access Grants Région AWS par compte. L'instance d'autorisations d'accès S3 sert de conteneur pour vos ressources d'autorisations d'accès S3, qui incluent les emplacements enregistrés et les octrois.

Avec S3 Access Grants, vous pouvez créer des autorisations pour vos données S3 pour les utilisateurs et les rôles AWS Identity and Access Management (IAM). Si vous avez ajouté votre répertoire d'identité d'entreprise à AWS IAM Identity Center, vous pouvez associer cette instance IAM Identity Center de votre répertoire d'entreprise à votre instance S3 Access Grants. Une fois que vous avez fait cela, vous pouvez créer des autorisations d'accès pour les utilisateurs et les groupes de votre entreprise. Si vous n'avez pas encore ajouté votre annuaire d'entreprise à IAM Identity Center, vous pouvez associer ultérieurement votre instance d'autorisations d'accès S3 à une instance IAM Identity Center.

Rubriques

- Création d'une instance d'autorisations d'accès S3
- Obtention des détails d'une instance d'autorisations d'accès S3
- Répertorier vos instances d'autorisations d'accès S3

- Association ou dissociation de votre instance IAM Identity Center
- Suppression d'une instance d'autorisations d'accès S3

Création d'une instance d'autorisations d'accès S3

Pour commencer à utiliser les octrois d'accès Amazon S3, vous devez d'abord créer une instance d'octrois d'accès S3. Vous ne pouvez créer qu'une seule instance S3 Access Grants Région AWS par compte. L'instance d'autorisations d'accès S3 sert de conteneur pour vos ressources d'autorisations d'accès S3, qui incluent les emplacements enregistrés et les octrois.

Avec S3 Access Grants, vous pouvez créer des autorisations pour vos données S3 pour les utilisateurs et les rôles AWS Identity and Access Management (IAM). Si vous avez ajouté votre répertoire d'identité d'entreprise à AWS IAM Identity Center, vous pouvez associer cette instance IAM Identity Center de votre répertoire d'entreprise à votre instance S3 Access Grants. Une fois que vous avez fait cela, vous pouvez créer des autorisations d'accès pour les utilisateurs et les groupes de votre entreprise. Si vous n'avez pas encore ajouté votre annuaire d'entreprise à IAM Identity Center, vous pouvez associer ultérieurement votre instance d'autorisations d'accès S3 à une instance IAM Identity Center.

Vous pouvez créer une instance S3 Access Grants en utilisant la console Amazon S3, le AWS Command Line Interface (AWS CLI), l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Avant de pouvoir accorder l'accès à vos données S3 avec S3 Access Grants, vous devez d'abord créer une instance S3 Access Grants Région AWS identique à vos données S3.

Prérequis

Si vous souhaitez accorder l'accès à vos données S3 en utilisant les identités de votre annuaire d'entreprise, ajoutez votre annuaire d'identités d'entreprise à AWS IAM Identity Center. Si vous n'êtes pas encore prêt à le faire, vous pouvez associer ultérieurement votre instance d'autorisations d'accès S3 à une instance IAM Identity Center.

Pour créer une instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région à laquelle vous souhaitez passer.

3. Dans le volet de navigation de gauche, choisissez Access Grants.
4. Sur la page Autorisations d'accès S3, choisissez Créer une instance d'autorisations d'accès S3.

   a. À l'étape 1 de l'Assistant Mise en place de l'instance Access Grants, vérifiez que vous souhaitez créer l'instance dans la Région AWS actuelle. Assurez-vous qu'il s'agit du même Région AWS endroit où se trouvent vos données S3. Vous pouvez créer une instance S3 Access Grants Région AWS par compte.

   b. (Facultatif) Si vous avez ajouté votre répertoire d'identité d'entreprise à AWS IAM Identity Center, vous pouvez associer cette instance IAM Identity Center de votre répertoire d'entreprise à votre instance S3 Access Grants.

      Pour ce faire, sélectionnez Ajouter une instance IAM Identity Center dans ***region***. Entrez ensuite l'Amazon Resource Name (ARN) de l'instance IAM Identity Center.

      Si vous n'avez pas encore ajouté votre annuaire d'entreprise à IAM Identity Center, vous pouvez associer ultérieurement votre instance d'octrois d'accès S3 à une instance IAM Identity Center.

   c. Pour créer l'instance d'autorisations d'accès S3, choisissez Suivant. Pour enregistrer un emplacement, consultez Étape 2 : enregistrer un emplacement.
5. Si l'option Suivant ou Créer une instance d'autorisations d'accès S3 est désactivée :

   Impossible de créer une instance

   - Vous avez peut-être déjà une instance d'autorisations d'accès S3 dans la même Région AWS. Dans le volet de navigation de gauche, choisissez Access Grants. Sur la page Autorisations d'accès S3, faites défiler la page vers le bas jusqu'à la section Instance d'autorisations d'accès S3 dans votre compte pour déterminer si une instance existe déjà.
   - Vous n'avez peut-être pas l'autorisation `s3:CreateAccessGrantsInstance` requise pour créer une instance d'autorisations d'accès S3. Contactez l'administrateur de votre compte. Pour les autorisations supplémentaires requises si vous associez une instance IAM Identity Center à votre instance d'autorisations d'accès S3, consultez CreateAccessGrantsInstance.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example Création d'une instance d'octrois d'accès S3

```
aws s3control create-access-grants-instance \
--account-id 111122223333 \
--region us-east-2
```

Réponse :

```
{
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00",
    "AccessGrantsInstanceId": "default",
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
}
```

Utilisation de l'API REST

Vous pouvez utiliser l'API REST Amazon S3 pour créer une instance d'autorisations d'accès S3. Pour plus d'informations sur la prise en charge de l'API REST pour la gestion d'une instance d'autorisations d'accès S3, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- AssociateAccessGrantsIdentityCenter
- CreateAccessGrantsInstance
- DeleteAccessGrantsInstance
- DissociateAccessGrantsIdentityCenter
- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix
- GetAccessGrantsInstanceResourcePolicy
- ListAccessGrantsInstances
- PutAccessGrantsInstanceResourcePolicy

En utilisant le AWS SDKs

Cette section fournit un exemple de création d'une instance S3 Access Grants à l'aide du AWS SDKs.

Java

Cet exemple crée l'instance d'autorisations d'accès S3, qui sert de conteneur pour vos autorisations d'accès individuelles. Vous pouvez avoir une instance S3 Access Région AWS Grants par compte. La réponse inclut l'ID de l'instance `default` et un Amazon Resource Name (ARN) généré pour votre instance d'autorisations d'accès S3.

Example Création d'une demande d'instance d'autorisations d'accès S3

```
public void createAccessGrantsInstance() {
CreateAccessGrantsInstanceRequest createRequest =
 CreateAccessGrantsInstanceRequest.builder().accountId("111122223333").build();
CreateAccessGrantsInstanceResponse createResponse =
 s3Control.createAccessGrantsInstance(createRequest);LOGGER.info("CreateAccessGrantsInstance
 " + createResponse);
}
```

Réponse :

```
CreateAccessGrantsInstanceResponse(
CreatedAt=2023-06-07T01:46:20.507Z,
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default)
```

Obtention des détails d'une instance d'autorisations d'accès S3

Vous pouvez consulter les détails de votre instance d'autorisations d'accès Amazon S3 dans une Région AWS particulière. Vous pouvez obtenir les détails de votre instance S3 Access Grants en utilisant la console Amazon S3, le AWS Command Line Interface (AWS CLI), l'API REST Amazon S3 et le AWS SDKs.

Utilisation de la console S3

Pour obtenir les détails d'une instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.

4. La page Autorisations d'accès S3 répertorie vos instances d'autorisations d'accès S3 et toutes les instances entre comptes qui ont été partagées avec votre compte. Pour visualiser les détails d'une instance, choisissez Afficher les détails.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Obtenir les détails d'une instance d'autorisations d'accès S3

```
aws s3control get-access-grants-instance \
 --account-id 111122223333 \
 --region us-east-2
```

Réponse :

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la gestion d'une instance d'autorisations d'accès S3, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- GetAccessGrantsInstance
- GetAccessGrantsInstanceForPrefix

En utilisant le AWS SDKs

Cette section fournit des exemples de la manière d'obtenir les détails d'une instance S3 Access Grants à l'aide du AWS SDKs.

Pour utiliser les exemples suivants, remplacez *user input placeholders* par vos propres informations.

Java

Example : Obtenir une instance d'autorisations d'accès S3

```
public void getAccessGrantsInstance() {
GetAccessGrantsInstanceRequest getRequest = GetAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
GetAccessGrantsInstanceResponse getResponse =
 s3Control.getAccessGrantsInstance(getRequest);
LOGGER.info("GetAccessGrantsInstanceResponse: " + getResponse);
}
```

Réponse :

```
GetAccessGrantsInstanceResponse(
AccessGrantsInstanceArn=arn:aws:s3:us-east-2: 111122223333:access-grants/default,
CreatedAt=2023-06-07T01:46:20.507Z)
```

Répertorier vos instances d'autorisations d'accès S3

Vous pouvez répertorier vos instances S3 Access Grants, y compris les instances qui ont été partagées avec vous via AWS Resource Access Manager (AWS RAM).

Vous pouvez répertorier vos instances S3 Access Grants à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et du AWS SDKs.

Utilisation de la console S3

Pour répertorier vos instances d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.

4. La page Autorisations d'accès S3 répertorie vos instances d'autorisations d'accès S3 et toutes les instances entre comptes qui ont été partagées avec votre compte. Pour visualiser les détails d'une instance, choisissez Afficher les détails.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Répertorier toutes les instances d'autorisations d'accès S3 pour un compte

Cette action répertorie les instances d'autorisations d'accès S3 pour un compte. Vous ne pouvez avoir qu'une seule instance S3 Access Grants par instance Région AWS. Cette action répertorie également les autres instances d'autorisations d'accès S3 entre comptes auxquelles votre compte a accès.

```
aws s3control list-access-grants-instances \
 --account-id 111122223333 \
 --region us-east-2
```

Réponse :

```
{
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default",
    "AccessGrantsInstanceId": "default",
    "CreatedAt": "2023-05-31T17:54:07.893000+00:00"
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la gestion d'une instance d'autorisations d'accès S3, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- ListAccessGrantsInstances

En utilisant le AWS SDKs

Cette section fournit des exemples de la manière d'obtenir les détails d'une instance S3 Access Grants à l'aide du AWS SDKs.

Pour utiliser les exemples suivants, remplacez *user input placeholders* par vos propres informations.

Java

Example : Répertorier toutes les instances d'autorisations d'accès S3 pour un compte

Cette action répertorie les instances d'octrois d'accès S3 pour un compte. Vous ne pouvez disposer que d'une seule instance d'autorisations d'accès S3 par région. Cette action peut également répertorier d'autres instances d'autorisations d'accès S3 entre comptes auxquelles votre compte a accès.

```
public void listAccessGrantsInstances() {
ListAccessGrantsInstancesRequest listRequest =
 ListAccessGrantsInstancesRequest.builder()
.accountId("111122223333")
.build();
ListAccessGrantsInstancesResponse listResponse =
 s3Control.listAccessGrantsInstances(listRequest);
LOGGER.info("ListAccessGrantsInstancesResponse: " + listResponse);
}
```

Réponse :

```
ListAccessGrantsInstancesResponse(
AccessGrantsInstancesList=[
ListAccessGrantsInstanceEntry(
AccessGrantsInstanceId=default,
AccessGrantsInstanceArn=arn:aws:s3:us-east-2:111122223333:access-grants/default,
CreatedAt=2023-06-07T04:28:11.728Z
)
]
)
```

Association ou dissociation de votre instance IAM Identity Center

Dans Amazon S3 Access Grants, vous pouvez associer l' AWS IAM Identity Center instance de votre répertoire d'identité d'entreprise à une instance S3 Access Grants. Ensuite, vous pouvez créer des autorisations d'accès pour les utilisateurs et les groupes de votre annuaire d'entreprise, en plus des utilisateurs et des rôles AWS Identity and Access Management (IAM).

Si vous ne souhaitez plus créer d'autorisations d'accès pour les utilisateurs et les groupes de votre annuaire d'entreprise, vous pouvez dissocier votre instance IAM Identity Center de votre instance d'autorisations d'accès S3.

Vous pouvez associer ou dissocier une instance IAM Identity Center à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et du. AWS SDKs

Utilisation de la console S3

Avant d'associer votre instance IAM Identity Center à votre instance d'autorisations d'accès S3, vous devez ajouter votre annuaire d'identités d'entreprise à IAM Identity Center. Pour plus d'informations, consultez the section called "Autorisations d'accès S3 et identités d'annuaire d'entreprise".

Pour associer une instance IAM Identity Center à une instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.
4. Choisissez Afficher les détails pour cette instance.
5. Sur la page de détails, dans la section IAM Identity Center, choisissez Ajouter pour ajouter une instance IAM Identity Center ou Désenregistrer pour annuler l'enregistrement d'une instance IAM Identity Center déjà associée.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Associer une instance IAM Identity Center à une instance d'autorisations d'accès S3

```
aws s3control associate-access-grants-identity-center \
 --account-id 111122223333 \
 --identity-center-arn arn:aws:sso:::instance/ssoins-1234a567bb89012c \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

Example : Dissocier une instance IAM Identity Center d'une instance d'autorisations d'accès S3

```
aws s3control dissociate-access-grants-identity-center \
 --account-id 111122223333 \
 --profile access-grants-profile \
 --region eu-central-1

// No response body
```

Utilisation de l'API REST

Pour en savoir plus sur la prise en charge de l'API REST Amazon S3 pour la gestion de l'association entre une instance IAM Identity Center et une instance d'autorisations d'accès S3, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- AssociateAccessGrantsIdentityCenter
- DissociateAccessGrantsIdentityCenter

Suppression d'une instance d'autorisations d'accès S3

Vous pouvez supprimer une instance Amazon S3 Access Grants depuis un Région AWS compte. Toutefois, avant de supprimer une instance d'autorisations d'accès S3, vous devez effectuer les opérations suivantes :

- Supprimez toutes les ressources figurant dans l'instance d'autorisations d'accès S3, y compris tous les octrois et tous les emplacements. Pour plus d'informations, consultez Suppression d'un octroi et Suppression d'un emplacement.
- Si vous avez associé une AWS IAM Identity Center instance à votre instance S3 Access Grants, vous devez dissocier l'instance IAM Identity Center. Pour plus d'informations, consultez Association ou dissociation de votre instance IAM Identity Center.

> **Important**
>
> Si vous supprimez une instance d'autorisations d'accès S3, la suppression est permanente et ne peut pas être annulée. Tous les bénéficiaires auxquels l'accès a été accordé via les octrois figurant dans cette instance d'autorisations d'accès S3 perdront l'accès à vos données S3.

Vous pouvez supprimer une instance S3 Access Grants à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et du AWS SDKs.

Utilisation de la console S3

Pour supprimer une instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.
4. Choisissez Afficher les détails pour cette instance.
5. Sur la page de détails de l'instance, choisissez Supprimer une instance dans le coin supérieur droit.
6. Dans la boîte de dialogue qui s'affiche, choisissez Supprimer. Cette action ne peut pas être annulée.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *`user input placeholders`* par vos propres informations.

> **Note**
>
> Avant de pouvoir supprimer une instance d'autorisations d'accès S3, vous devez d'abord supprimer tous les octrois et tous les emplacements créés dans l'instance d'autorisations

d'accès S3. Si vous avez associé une instance du centre IAM Identity Center à votre instance d'autorisations d'accès S3, vous devez d'abord l'en dissocier.

Example : Supprimer une instance d'autorisations d'accès S3

```
aws s3control delete-access-grants-instance \
--account-id 111122223333 \
--profile access-grants-profile \
--region us-east-2 \
--endpoint-url https://s3-control.us-east-2.amazonaws.com \

 // No response body
```

Utilisation de l'API REST

Pour en savoir plus sur la prise en charge de l'API REST Amazon S3 pour la suppression d'une instance d'autorisations d'accès S3, consultez DeleteAccessGrantsInstance dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Cette section fournit des exemples de suppression d'une instance S3 Access Grants à l'aide du AWS SDKs.

Pour utiliser l'exemple suivant, remplacez les *user input placeholders* par vos propres informations.

Java

> **Note**
>
> Avant de pouvoir supprimer une instance d'octrois d'accès S3, vous devez d'abord supprimer tous les octrois et tous les emplacements créés dans l'instance d'octrois d'accès S3. Si vous avez associé une instance du centre IAM Identity Center à votre instance d'autorisations d'accès S3, vous devez d'abord l'en dissocier.

Example : Supprimer une instance d'autorisations d'accès S3

```
public void deleteAccessGrantsInstance() {
```

```
DeleteAccessGrantsInstanceRequest deleteRequest =
 DeleteAccessGrantsInstanceRequest.builder()
.accountId("111122223333")
.build();
DeleteAccessGrantsInstanceResponse deleteResponse =
 s3Control.deleteAccessGrantsInstance(deleteRequest);
LOGGER.info("DeleteAccessGrantsInstanceResponse: " + deleteResponse);
}
```

Utilisation des emplacements d'autorisations d'accès S3

Après avoir créé une instance Amazon S3 Access Grants Région AWS dans un compte, vous enregistrez un emplacement S3 dans cette instance. Un emplacement S3 Access Grants associe l'emplacement S3 par défaut (`s3://`), un compartiment ou un préfixe à un rôle AWS Identity and Access Management (IAM). Les autorisations d'accès S3 endosseront ce rôle IAM pour fournir des informations d'identification temporaires au bénéficiaire qui accédera à cet emplacement particulier. Vous devez d'abord enregistrer au moins un emplacement auprès de votre instance d'autorisations d'accès S3 avant de pouvoir créer des autorisations d'accès.

Vous pouvez enregistrer un emplacement, en consulter les détails, le modifier ou le supprimer.

> **Note**
>
> Une fois que vous avez enregistré le premier emplacement dans votre instance d'autorisations d'accès S3, celle-ci ne dispose toujours d'aucune autorisation d'accès individuelle. Pour créer une autorisation d'accès, consultez Création d'octrois.

Rubriques

- Enregistrement d'un emplacement
- Affichage des détails d'un emplacement enregistré
- Mise à jour d'un emplacement enregistré
- Suppression d'un emplacement enregistré

Enregistrement d'un emplacement

Après avoir créé une instance Amazon S3 Access Grants Région AWS dans un compte, vous enregistrez un emplacement S3 dans cette instance. Un emplacement S3 Access Grants associe l'emplacement S3 par défaut (`s3://`), un compartiment ou un préfixe à un rôle AWS Identity and Access Management (IAM). Les autorisations d'accès S3 endosseront ce rôle IAM pour fournir des informations d'identification temporaires au bénéficiaire qui accédera à cet emplacement particulier. Vous devez d'abord enregistrer au moins un emplacement auprès de votre instance d'autorisations d'accès S3 avant de pouvoir créer des autorisations d'accès.

Cas d'utilisation recommandé

Nous vous recommandons d'enregistrer l'emplacement par défaut (`s3://`) et de le mapper à un rôle IAM. L'emplacement sur le chemin S3 par défaut (`s3://`) couvre l'accès à tous vos compartiments S3 dans celui Région AWS de votre compte. Lorsque vous créez une autorisation d'accès, vous pouvez restreindre la portée de cette autorisation à un compartiment, à un préfixe ou à un objet situé à l'emplacement par défaut.

Cas d'utilisation complexes de gestion des accès

Les cas d'utilisation plus complexes liés à la gestion des accès peuvent vous obliger à enregistrer un autre emplacement que l'emplacement par défaut. Voici quelques exemples de tels cas d'utilisation :

- Supposons qu'*`amzn-s3-demo-bucket`* soit un emplacement enregistré dans votre instance d'autorisations d'accès S3 et qu'un rôle IAM lui soit associé, mais que ce rôle IAM se voit refuser l'accès à un préfixe particulier dans le compartiment. Dans ce cas, vous pouvez enregistrer le préfixe auquel le rôle IAM n'a pas accès en tant qu'emplacement distinct et associer cet emplacement à un autre rôle IAM disposant de l'accès nécessaire.
- Supposons que vous souhaitiez créer des autorisations qui limitent l'accès aux utilisateurs au sein d'un point de terminaison de cloud privé virtuel (VPC). Dans ce cas, vous pouvez enregistrer un emplacement pour un compartiment dans lequel le rôle IAM restreint l'accès à ce point de terminaison du VPC. Ultérieurement, lorsqu'un bénéficiaire demandera des informations d'identification aux autorisations d'accès S3, les autorisations d'accès S3 endosseront le rôle IAM de l'emplacement pour fournir des informations d'identification temporaires. Ces informations d'identification refuseront l'accès au compartiment spécifique, sauf si l'appelant se trouve dans le point de terminaison du VPC. Cette autorisation de refus sera appliquée en plus de l'autorisation READ, WRITE ou READWRITE habituellement spécifiée dans l'autorisation d'accès.

Lorsque vous enregistrez un emplacement, vous devez également spécifier le rôle IAM que les autorisations d'accès S3 endossent pour fournir des informations d'identification temporaires et délimiter la portée d'une autorisation spécifique.

Si votre cas d'utilisation vous oblige à enregistrer plusieurs emplacements dans votre instance d'autorisations d'accès S3, vous pouvez enregistrer l'un des emplacements suivants :

URI S3	Rôle IAM	Description
`s3://`	*`Default-IAM-role`*	L'emplacement par défaut, `s3://`, inclut tous les compartiments figurant dans la Région AWS.
`s3://`*`amzn-s3-demo-bucket1`*`/`	*`IAM-role-For-bucket`*	Cet emplacement inclut tous les objets figurant dans le compartiment spécifié.
`s3://`*`amzn-s3-demo-bucket1`*`/`*`prefix-name`*	*`IAM-role-For-prefix`*	Cet emplacement inclut tous les objets du compartiment dont le nom de clé d'objet commence par ce préfixe.

Avant de pouvoir enregistrer un compartiment ou un préfixe spécifique, assurez-vous d'effectuer les opérations suivantes :

- Créez un ou plusieurs compartiments contenant les données auxquelles vous souhaitez accorder l'accès. Ces compartiments doivent être situés au même endroit Région AWS que votre instance S3 Access Grants. Pour de plus amples informations, veuillez consulter Créer un compartiment.

  L'ajout d'un préfixe est une étape facultative. Les préfixes sont les chaînes qui se trouvent au début du nom de la clé d'objet. Vous pouvez les utiliser pour organiser les objets dans votre compartiment ainsi que pour gérer les accès. Pour ajouter un préfixe à un compartiment, consultez Création de noms de clés d'objets.
- Créez un rôle IAM qui dispose de l'autorisation nécessaire pour accéder à vos données S3 dans la Région AWS. Pour plus d'informations, consultez Création de rôles IAM dans le Guide de l'utilisateur AWS IAM Identity Center .
- Dans la politique de confiance du rôle IAM, accordez au service d'autorisations d'accès S3 (`access-grants.s3.amazonaws.com`) l'accès au rôle IAM que vous avez créé. Pour ce faire, vous pouvez créer un fichier JSON contenant les instructions suivantes. Pour ajouter la politique

d'approbation à votre compte, consultez Création d'un rôle à l'aide de politiques d'approbation personnalisées.

TestRolePolicy.json

JSON

```
{
  "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "TestRolePolicy",
      "Effect": "Allow",
      "Principal": {
        "Service":"access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount":"accountId",
          "aws:SourceArn":"arn:aws:s3:region:accountId:access-grants/default"
        }
      }
    }
  ]
}
```

Sinon, pour un cas d'utilisation d'IAM Identity Center, utilisez la politique suivante qui inclut une deuxième déclaration :

JSON

```
{
  "Version": "2012-10-17",
    "Statement": [
    {
      "Sid": "TestRolePolicyIdentityCenter",
      "Effect": "Allow",
```

```
      "Principal": {
        "Service":"access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount":"111122223333",
          "aws:SourceArn":"arn:aws:s3:aws-region:111122223333:access-grants/
default"
        }
      }
    },
    {
      "Sid": "Stmt1234567891012",
        "Effect": "Allow",
        "Principal": {
          "Service": "access-grants.s3.amazonaws.com"
        },
        "Action": "sts:SetContext",
        "Resource": "*",
        "Condition":{
          "StringEquals":{
            "aws:SourceAccount":"111122223333",
            "aws:SourceArn":"arn:aws:s3:aws-region:111122223333:access-grants/
default"
          },
          "ForAllValues:ArnEquals": {

 "sts:RequestContextProviders":"arn:aws:iam::111122223333:contextProvider/
IdentityCenter"
          }
        }
      }
  ]
}
```

- Créez une politique IAM pour attacher les autorisations Amazon S3 au rôle IAM que vous avez créé. Consultez l'exemple de fichier `iam-policy.json` suivant et remplacez les *`user input placeholders`* par vos propres informations.

> **Note**
>
> - Si vous utilisez le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) pour chiffrer vos données, l'exemple suivant inclut les AWS KMS autorisations nécessaires pour le rôle IAM dans la politique. Si vous n'utilisez pas cette fonctionnalité, vous pouvez supprimer ces autorisations de votre politique IAM.
> - Vous pouvez faire en sorte que le rôle IAM ne puisse accéder aux données S3 que si les informations d'identification sont fournies par les autorisations d'accès S3. Cet exemple montre comment ajouter une instruction `Condition` pour une instance d'autorisations d'accès S3 spécifique. Pour utiliser cette `Condition`, remplacez l'ARN de l'instance d'autorisations d'accès S3 dans l'instruction `Condition` par l'ARN de votre instance d'autorisations d'accès S3, au format suivant : `arn:aws:s3:`*`region`*`:`*`accountId`*`:access-grants/default`

iam-policy.json

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
         "Sid": "ObjectLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:GetObjectAcl",
            "s3:GetObjectVersionAcl",
            "s3:ListMultipartUploadParts"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
```

```
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:region:accountId:access-
grants/default"]
            }
        }
      },
      {
         "Sid": "ObjectLevelWritePermissions",
         "Effect":"Allow",
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:PutObjectVersionAcl",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Région
 AWS:accountId:access-grants/default"]
            }
         }
      },
      {
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:Région
 AWS:accountId:access-grants/default"]
            }
         }
```

```
      },
   //Optionally add the following section if you use SSE-KMS encryption
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
}
```

Vous pouvez enregistrer un emplacement dans votre instance S3 Access Grants à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 ou du AWS SDKs.

> **Note**
>
> Une fois que vous avez enregistré le premier emplacement dans votre instance d'autorisations d'accès S3, celle-ci ne dispose toujours d'aucune autorisation d'accès individuelle. Pour créer une autorisation d'accès, consultez Création d'octrois.

Utilisation de la console S3

Avant de pouvoir accorder l'accès à vos données S3 avec les autorisations d'accès S3, vous devez avoir au moins un emplacement enregistré.

Pour enregistrer un emplacement dans votre instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.

Si vous utilisez une instance d'autorisations d'accès S3 pour la première fois, assurez-vous d'avoir terminé l'étape 1 : Créer une instance d'autorisations d'accès S3 et d'être passé à l'étape 2 de l'Assistant Mise en place de l'instance Access Grants. Si vous possédez déjà une instance d'autorisations d'accès S3, choisissez Afficher les détails, puis, dans l'onglet Succursales, choisissez Enregistrer l'emplacement.

a. Pour Champ d'application de l'emplacement, choisissez Parcourir S3 ou entrez le chemin d'URI S3 menant à l'emplacement que vous souhaitez enregistrer. Pour les formats d'URI S3, consultez le tableau des formats d'emplacement. Après avoir entré un URI, vous pouvez choisir Afficher pour accéder à l'emplacement.

b. Pour Rôle IAM choisissez l'une des options suivantes :

   - Sélectionner parmi les rôles IAM existants

     Choisissez un rôle IAM dans la liste déroulante. Après avoir choisi un rôle, choisissez Afficher pour vous assurer que ce rôle dispose des autorisations nécessaires pour gérer l'emplacement que vous enregistrez. Plus précisément, assurez-vous que ce rôle accorde aux autorisations d'accès S3 les autorisations `sts:AssumeRole` et `sts:SetSourceIdentity`.

   - Saisir l'ARN du rôle IAM

     Accédez à la console IAM. Copiez l'Amazon Resource Name (ARN) du rôle IAM et collez-le dans cette zone.

c. Pour terminer, choisissez Suivant ou Enregistrer l'emplacement.

4. Résolution des problèmes :

   Impossible d'enregistrer l'emplacement

   - L'emplacement est peut-être déjà enregistré.

     Il se peut que vous n'ayez pas l'autorisation `s3:CreateAccessGrantsLocation` d'enregistrer des emplacements. Contactez l'administrateur de votre compte.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Vous pouvez enregistrer l'emplacement par défaut, `s3://`, ou un emplacement personnalisé dans votre instance d'autorisations d'accès S3. Assurez-vous d'abord de créer un rôle IAM avec un accès principal à l'emplacement, puis d'accorder aux autorisations d'accès S3 l'autorisation d'endosser ce rôle.

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

Example Créer une politique de ressources

Créez une politique permettant aux autorisations d'accès S3 d'endosser le rôle IAM. Pour ce faire, vous pouvez créer un fichier JSON contenant les instructions suivantes. Pour ajouter la politique de ressources à votre compte, consultez Créer et attacher votre première politique gérée par le client.

TestRolePolicy.json

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Action": ["sts:AssumeRole", "sts:SetSourceIdentity"],
      "Effect": "Allow",
      "Principal": {"Service":"access-grants.s3.amazonaws.com"},
      "Resource": "*"
    }
  ]
}
```

Example Créer le rôle

Exécutez la commande IAM suivante pour créer le rôle.

```
aws iam create-role --role-name accessGrantsTestRole \
 --region us-east-2 \
 --assume-role-policy-document file://TestRolePolicy.json
```

L'exécution de la commande `create-role` renvoie la politique :

```
{
    "Role": {
        "Path": "/",
        "RoleName": "accessGrantsTestRole",
        "RoleId": "AROASRDGX4WM4GH55GIDA",
        "Arn": "arn:aws:iam::111122223333:role/accessGrantsTestRole",
        "CreateDate": "2023-05-31T18:11:06+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Sid": "Stmt1685556427189",
                    "Action": [
                        "sts:AssumeRole",
                        "sts:SetSourceIdentity"
                    ],
                    "Effect": "Allow",
                    "Principal": {
                        "Service":"access-grants.s3.amazonaws.com"
                    }
                }
            ]
        }
    }
}
```

Example

Créez une politique IAM pour attacher les autorisations Amazon S3 au rôle IAM. Consultez l'exemple de fichier `iam-policy.json` suivant et remplacez les *`user input placeholders`* par vos propres informations.

> **Note**
>
> Si vous utilisez le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) pour chiffrer vos données, l'exemple suivant ajoute les AWS KMS autorisations nécessaires pour le rôle IAM dans la politique. Si vous n'utilisez pas cette fonctionnalité, vous pouvez supprimer ces autorisations de votre politique IAM.
>
> Pour vous assurer que le rôle IAM ne peut être utilisé que pour accéder aux données dans S3 si les informations d'identification sont proposées par les autorisations d'accès S3, cet

exemple vous montre comment ajouter une déclaration `Condition` spécifiant l'instance d'autorisations d'accès S3 (`s3:AccessGrantsInstance: InstanceArn`) dans votre politique IAM. Lorsque vous utilisez l'exemple de politique suivant, remplacez les *user input placeholders* par vos propres informations.

iam-policy.json

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
       {
         "Sid": "ObjectLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion",
            "s3:GetObjectAcl",
            "s3:GetObjectVersionAcl",
            "s3:ListMultipartUploadParts"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "accountId" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn":
 ["arn:aws:s3:region:accountId:access-grants/default"]
            }
       }
     },
     {
        "Sid": "ObjectLevelWritePermissions",
        "Effect":"Allow",
        "Action":[
           "s3:PutObject",
           "s3:PutObjectAcl",
           "s3:PutObjectVersionAcl",
```

```
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:AbortMultipartUpload"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "111122223333" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:aws-
region:111122223333:access-grants/default"]
            }
         }
      },
      {
         "Sid": "BucketLevelReadPermissions",
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::*"
         ],
         "Condition":{
            "StringEquals": { "aws:ResourceAccount": "111122223333" },
            "ArnEquals": {
                "s3:AccessGrantsInstanceArn": ["arn:aws:s3:aws-
region:111122223333:access-grants/default"]
            }
         }
      },
      {
         "Sid": "KMSPermissions",
         "Effect":"Allow",
         "Action":[
            "kms:Decrypt",
            "kms:GenerateDataKey"
         ],
         "Resource":[
            "*"
         ]
      }
   ]
```

```
}
```

Example

Exécutez la commande suivante :

```
aws iam put-role-policy \
--role-name accessGrantsTestRole \
--policy-name accessGrantsTestRole \
--policy-document file://iam-policy.json
```

Example Enregistrer l'emplacement par défaut

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3:// \
 --iam-role-arn arn:aws:iam::111122223333:role/accessGrantsTestRole
```

Réponse :

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example Enregistrer un emplacement personnalisé

```
aws s3control create-access-grants-location \
 --account-id 111122223333 \
 --location-scope s3://DOC-BUCKET-EXAMPLE/ \
 --iam-role-arn arn:aws:iam::123456789012:role/accessGrantsTestRole
```

Réponse :

```
{"CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
```

```
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2: 111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://DOC-BUCKET-EXAMPLE/",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la gestion d'une instance d'autorisations d'accès S3, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- CreateAccessGrantsLocation
- DeleteAccessGrantsLocation
- GetAccessGrantsLocation
- ListAccessGrantsLocations
- UpdateAccessGrantsLocation

En utilisant le AWS SDKs

Cette section fournit des exemples de la manière d'enregistrer des emplacements à l'aide du AWS SDKs.

Pour utiliser les exemples suivants, remplacez *user input placeholders* par vos propres informations.

Java

Vous pouvez enregistrer l'emplacement par défaut, `s3://`, ou un emplacement personnalisé dans votre instance d'octrois d'accès S3. Assurez-vous d'abord de créer un rôle IAM avec un accès principal à l'emplacement, puis d'accorder aux autorisations d'accès S3 l'autorisation d'endosser ce rôle.

Pour utiliser les exemples de commandes suivants, remplacez les *user input placeholders* par vos propres informations.

Example Enregistrer un emplacement par défaut

Requête :

```
public void createAccessGrantsLocation() {
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://")
.iamRoleArn("arn:aws:iam::123456789012:role/accessGrantsTestRole")
.build();
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

Réponse :

```
CreateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example Enregistrer un emplacement personnalisé

Requête :

```
public void createAccessGrantsLocation() {
CreateAccessGrantsLocationRequest createRequest =
 CreateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.locationScope("s3://DOC-BUCKET-EXAMPLE/")
.iamRoleArn("arn:aws:iam::111122223333:role/accessGrantsTestRole")
.build();
CreateAccessGrantsLocationResponse createResponse =
 s3Control.createAccessGrantsLocation(createRequest);
LOGGER.info("CreateAccessGrantsLocationResponse: " + createResponse);
}
```

Réponse :

```
CreateAccessGrantsLocationResponse(
```

```
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=18cfe6fb-eb5a-4ac5-aba9-8d79f04c2012,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/18cfe6fb-eb5a-4ac5-aba9-8d79f04c2666,
LocationScope= s3://test-bucket-access-grants-user123/,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Affichage des détails d'un emplacement enregistré

Vous pouvez obtenir les détails d'un emplacement enregistré dans votre instance S3 Access Grants en utilisant la console Amazon S3, le AWS Command Line Interface (AWS CLI), l'API REST Amazon S3 et le AWS SDKs.

Utilisation de la console S3

Pour afficher les emplacements enregistrés dans votre instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.
4. Choisissez Afficher les détails pour cette instance.
5. Sur la page de détails de l'instance, choisissez l'onglet Succursales.
6. Recherchez l'emplacement enregistré que vous souhaitez afficher. Pour filtrer la liste des emplacements enregistrés, utilisez la zone de recherche.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Obtenir les détails d'un emplacement enregistré

```
aws s3control get-access-grants-location \
```

```
--account-id 111122223333 \
--access-grants-location-id default
```

Réponse :

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
}
```

Example : Répertorier tous les emplacements enregistrés dans une instance d'autorisations d'accès S3

Pour limiter les résultats à un préfixe ou à un compartiment S3, vous pouvez éventuellement utiliser le paramètre `--location-scope s3://bucket-and-or-prefix`.

```
aws s3control list-access-grants-locations \
--account-id 111122223333 \
--region us-east-2
```

Réponse :

```
{"AccessGrantsLocationsList": [
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "default",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/default",
    "LocationScope": "s3://"
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     },
  {
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb456",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixA*",
    "IAMRoleArn": "arn:aws:iam::111122223333:role/accessGrantsTestRole"
     }
```

```
 ]
}
```

Utilisation de l'API REST

Pour en savoir plus sur la prise en charge de l'API REST Amazon S3 pour obtenir les détails d'un emplacement enregistré ou répertorier tous les emplacements enregistrés auprès d'une instance d'autorisations d'accès S3, consultez les sections suivantes de la Référence d'API Amazon Simple Storage Service :

- GetAccessGrantsLocation
- ListAccessGrantsLocations

En utilisant le AWS SDKs

Cette section fournit des exemples de la façon d'obtenir les détails d'un emplacement enregistré ou de répertorier tous les emplacements enregistrés dans une instance S3 Access Grants à l'aide du AWS SDKs.

Pour utiliser les exemples suivants, remplacez *user input placeholders* par vos propres informations.

Java

Example : Obtenir les détails d'un emplacement enregistré

```
public void getAccessGrantsLocation() {
GetAccessGrantsLocationRequest getAccessGrantsLocationRequest =
 GetAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("default")
.build();
GetAccessGrantsLocationResponse getAccessGrantsLocationResponse =
 s3Control.getAccessGrantsLocation(getAccessGrantsLocationRequest);
LOGGER.info("GetAccessGrantsLocationResponse: " + getAccessGrantsLocationResponse);
}
```

Réponse :

```
GetAccessGrantsLocationResponse(
```

```
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope= s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
```

Example : Répertorier tous les emplacements enregistrés dans une instance d'autorisations d'accès S3

Pour limiter les résultats à un préfixe ou à un compartiment S3, vous pouvez éventuellement transmettre un URI S3, tel que `s3://bucket-and-or-prefix`, dans le paramètre `LocationScope`.

```
public void listAccessGrantsLocations() {

ListAccessGrantsLocationsRequest listRequest =
 ListAccessGrantsLocationsRequest.builder()
.accountId("111122223333")
.build();

ListAccessGrantsLocationsResponse listResponse =
 s3Control.listAccessGrantsLocations(listRequest);
LOGGER.info("ListAccessGrantsLocationsResponse: " + listResponse);
}
```

Réponse :

```
ListAccessGrantsLocationsResponse(
AccessGrantsLocationsList=[
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:11.027Z,
AccessGrantsLocationId=default,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/default,
LocationScope=s3://,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
),
ListAccessGrantsLocationsEntry(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb456,
```

```
AccessGrantsLocationArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixA*,
IAMRoleArn=arn:aws:iam::111122223333:role/accessGrantsTestRole
)
]
)
```

Mise à jour d'un emplacement enregistré

Vous pouvez mettre à jour le rôle AWS Identity and Access Management (IAM) d'un emplacement enregistré dans votre instance Amazon S3 Access Grants. Pour chaque nouveau rôle IAM que vous utilisez pour enregistrer un emplacement dans les autorisations d'accès S3, veillez à accorder au principal du service d'autorisations d'accès S3 (`access-grants.s3.amazonaws.com`) l'accès à ce rôle. Pour ce faire, ajoutez une entrée pour le nouveau rôle IAM dans le même fichier JSON de politique d'approbation que celui que vous avez utilisé quand vous avez enregistré l'emplacement pour la première fois.

Vous pouvez mettre à jour un emplacement dans votre instance S3 Access Grants à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et du AWS SDKs.

Utilisation de la console S3

Pour mettre à jour le rôle IAM d'un emplacement enregistré auprès de votre instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.
4. Choisissez Afficher les détails pour cette instance.
5. Sur la page de détails de l'instance, choisissez l'onglet Succursales.
6. Recherchez l'emplacement que vous souhaitez mettre à jour. Pour filtrer la liste des emplacements, utilisez la zone de recherche.
7. Choisissez le bouton d'options en regard de l'emplacement enregistré que vous voulez mettre à jour.

8. Mettez à jour le rôle IAM, puis choisissez Enregistrer les modifications.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Mettre à jour le rôle IAM d'un emplacement enregistré

```
aws s3control update-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id 635f1139-1af2-4e43-8131-a4de006eb999 \
--iam-role-arn arn:aws:iam::777788889999:role/accessGrantsTestRole
```

Réponse :

```
{
    "CreatedAt": "2023-05-31T18:23:48.107000+00:00",
    "AccessGrantsLocationId": "635f1139-1af2-4e43-8131-a4de006eb999",
    "AccessGrantsLocationArn": "arn:aws:s3:us-east-2:777788889999:access-grants/
default/location/635f1139-1af2-4e43-8131-a4de006eb888",
    "LocationScope": "s3://amzn-s3-demo-bucket/prefixB*",
    "IAMRoleArn": "arn:aws:iam::777788889999:role/accessGrantsTestRole"
}
```

Utilisation de l'API REST

Pour en savoir plus sur la prise en charge de l'API REST Amazon S3 pour la mise à jour d'un emplacement dans une instance d'autorisations d'accès S3, consultez UpdateAccessGrantsLocation dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Cette section fournit des exemples de mise à jour du rôle IAM d'un établissement enregistré à l'aide du AWS SDKs.

Pour utiliser l'exemple suivant, remplacez les *user input placeholders* par vos propres informations.

Java

Example : Mettre à jour le rôle IAM d'un emplacement enregistré

```
public void updateAccessGrantsLocation() {
UpdateAccessGrantsLocationRequest updateRequest =
 UpdateAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("635f1139-1af2-4e43-8131-a4de006eb999")
.iamRoleArn("arn:aws:iam::777788889999:role/accessGrantsTestRole")
.build();
UpdateAccessGrantsLocationResponse updateResponse =
 s3Control.updateAccessGrantsLocation(updateRequest);
LOGGER.info("UpdateAccessGrantsLocationResponse: " + updateResponse);
}
```

Réponse :

```
UpdateAccessGrantsLocationResponse(
CreatedAt=2023-06-07T04:35:10.027Z,
AccessGrantsLocationId=635f1139-1af2-4e43-8131-a4de006eb999,
AccessGrantsLocationArn=arn:aws:s3:us-east-2:777788889999:access-grants/default/
location/635f1139-1af2-4e43-8131-a4de006eb888,
LocationScope=s3://amzn-s3-demo-bucket/prefixB*,
IAMRoleArn=arn:aws:iam::777788889999:role/accessGrantsTestRole
)
```

Suppression d'un emplacement enregistré

Vous pouvez supprimer un enregistrement d'emplacement à partir d'une instance d'autorisations d'accès Amazon S3. La suppression de l'emplacement désenregistre ce dernier de l'instance d'autorisations d'accès S3.

Avant de pouvoir supprimer un enregistrement d'emplacement à partir d'une instance d'autorisations d'accès S3, vous devez supprimer tous les octrois associés à cet emplacement. Pour en savoir plus sur la suppression d'octrois, consultez Suppression d'un octroi.

Vous pouvez supprimer un emplacement dans votre instance S3 Access Grants à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et du AWS SDKs.

Utilisation de la console S3

Pour supprimer un enregistrement d'emplacement de votre instance d'autorisations d'accès S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.
4. Choisissez Afficher les détails pour cette instance.
5. Sur la page de détails de l'instance, choisissez l'onglet Succursales.
6. Recherchez l'emplacement que vous souhaitez mettre à jour. Pour filtrer la liste des emplacements, utilisez la zone de recherche.
7. Choisissez le bouton d'option en regard de l'emplacement enregistré que vous voulez supprimer.
8. Choisissez Deregister (Annuler l'enregistrement).
9. Une boîte de dialogue apparaît pour vous avertir que cette action ne peut pas être annulée. Pour supprimer l'emplacement, choisissez Désenregistrer.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Supprimer un enregistrement d'emplacement

```
aws s3control delete-access-grants-location \
--account-id 111122223333 \
--access-grants-location-id  a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
 // No response body
```

Utilisation de l'API REST

Pour en savoir plus sur la prise en charge de l'API REST Amazon S3 pour la suppression d'un emplacement à partir d'une instance d'autorisations d'accès S3, consultez DeleteAccessGrantsLocation dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Cette section fournit un exemple de suppression d'un emplacement à l'aide du AWS SDKs.

Pour utiliser l'exemple suivant, remplacez les *`user input placeholders`* par vos propres informations.

Java

Example : Supprimer un enregistrement d'emplacement

```
public void deleteAccessGrantsLocation() {
DeleteAccessGrantsLocationRequest deleteRequest =
 DeleteAccessGrantsLocationRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantsLocationResponse deleteResponse =
 s3Control.deleteAccessGrantsLocation(deleteRequest);
LOGGER.info("DeleteAccessGrantsLocationResponse: " + deleteResponse);
}
```

Réponse :

```
DeleteAccessGrantsLocationResponse()
```

Octroi d'autorisations avec les autorisations d'accès S3

Une autorisation d'accès individuelle dans une instance S3 Access Grants permet à une identité spécifique (un principal AWS Identity and Access Management (IAM), un utilisateur ou un groupe dans un annuaire d'entreprise d'accéder à un emplacement enregistré dans votre instance S3 Access Grants. Un emplacement associe des compartiments ou des préfixes à un rôle IAM. Les autorisations d'accès S3 endosseront ce rôle IAM pour fournir des informations d'identification temporaires aux bénéficiaires.

Après avoir enregistré au moins un emplacement dans votre instance d'autorisations d'accès S3, vous pouvez créer une autorisation d'accès.

Le bénéficiaire peut être un utilisateur ou un rôle IAM, ou encore un utilisateur ou un groupe provenant d'un annuaire. Un utilisateur d'annuaire est un utilisateur issu de votre annuaire

d'entreprise ou d'une source d'identité externe que vous avez associée à votre instance d'autorisations d'accès S3. Pour de plus amples informations, veuillez consulter Autorisations d'accès S3 et identités d'annuaire d'entreprise. Pour créer une autorisation pour un utilisateur ou un groupe spécifique à partir d'IAM Identity Center, recherchez le GUID utilisé par IAM Identity Center afin d'identifier cet utilisateur dans IAM Identity Center (par exemple, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`). Pour plus d'informations sur l'utilisation d'IAM Identity Center pour consulter les informations utilisateur, consultez Affichage des attributions des utilisateurs et des groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Vous pouvez accorder l'accès à un compartiment, à un préfixe ou à un objet. Dans Amazon S3, un préfixe est une chaîne de caractères située au début d'un nom de clé d'objet et qui sert à organiser les objets au sein d'un compartiment. Il peut s'agir de n'importe quelle chaîne de caractères autorisés, par exemple des noms de clé d'objet d'un compartiment commençant par le préfixe `engineering/`.

Rubriques

- Création d'octrois
- Affichage d'un octroi
- Suppression d'un octroi

Création d'octrois

Une autorisation d'accès individuelle dans une instance S3 Access Grants permet à une identité spécifique (un principal AWS Identity and Access Management (IAM), un utilisateur ou un groupe dans un annuaire d'entreprise d'accéder à un emplacement enregistré dans votre instance S3 Access Grants. Un emplacement associe des compartiments ou des préfixes à un rôle IAM. Les autorisations d'accès S3 endosseront ce rôle IAM pour fournir des informations d'identification temporaires aux bénéficiaires.

Après avoir enregistré au moins un emplacement dans votre instance d'autorisations d'accès S3, vous pouvez créer une autorisation d'accès.

Le bénéficiaire peut être un utilisateur ou un rôle IAM, ou encore un utilisateur ou un groupe provenant d'un annuaire. Un utilisateur d'annuaire est un utilisateur issu de votre annuaire d'entreprise ou d'une source d'identité externe que vous avez associée à votre instance d'autorisations d'accès S3. Pour de plus amples informations, veuillez consulter Autorisations d'accès S3 et identités d'annuaire d'entreprise. Pour créer une autorisation pour un utilisateur ou un groupe

spécifique à partir d'IAM Identity Center, recherchez le GUID utilisé par IAM Identity Center afin d'identifier cet utilisateur dans IAM Identity Center (par exemple, `a1b2c3d4-5678-90ab-cdef-EXAMPLE11111`). Pour plus d'informations sur l'utilisation d'IAM Identity Center pour consulter les informations utilisateur, consultez Affichage des attributions des utilisateurs et des groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Vous pouvez accorder l'accès à un compartiment, à un préfixe ou à un objet. Dans Amazon S3, un préfixe est une chaîne de caractères située au début d'un nom de clé d'objet et qui sert à organiser les objets au sein d'un compartiment. Il peut s'agir de n'importe quelle chaîne de caractères autorisés, par exemple des noms de clé d'objet d'un compartiment commençant par le préfixe `engineering/`.

Sous-préfixe

Lorsque vous accordez l'accès à un emplacement enregistré, vous pouvez utiliser le champ `Subprefix` pour restreindre l'étendue de l'accès à un sous-ensemble de cet emplacement. Si l'emplacement enregistré que vous choisissez pour l'autorisation est le chemin S3 par défaut (`s3://`), vous devez réduire la portée de cette autorisation. Vous ne pouvez pas créer d'autorisation d'accès pour l'emplacement par défaut (`s3://`), ce qui permettrait au bénéficiaire d'accéder à chaque compartiment d'une Région AWS. À la place, vous devez limiter la portée de l'autorisation à l'un des éléments suivants :

- Un compartiment : `s3://`*`bucket`*`/*`
- Un préfixe dans un compartiment : `s3://`*`bucket`*`/`*`prefix`*`*`
- Un préfixe dans un préfixe : `s3://`*`bucket`*`/`*`prefixA`*`/`*`prefixB`*`*`
- Un objet : `s3://`*`bucket`*`/`*`object-key-name`*

Si vous créez une autorisation d'accès dans laquelle l'emplacement enregistré est un compartiment, vous pouvez transmettre l'un des éléments suivants dans le champ `Subprefix` pour limiter la portée de cette autorisation :

- Un préfixe dans le compartiment : *`prefix`*`*`
- Un préfixe dans un préfixe : *`prefixA/prefixB`*`*`
- Un objet : `/`*`object-key-name`*

Une fois que vous avez créé l'autorisation, l'étendue de la subvention qui s'affiche dans la console Amazon S3 ou `GrantScope` qui est renvoyée dans la réponse API ou AWS Command Line Interface

(AWS CLI) est le résultat de la concaténation du chemin de localisation avec le. `Subprefix` Assurez-vous que ce chemin concaténé correspond bien au compartiment, au préfixe ou à l'objet S3 auquel vous souhaitez accorder l'accès.

> **Note**
>
> - Si vous devez créer une autorisation d'accès qui octroie l'accès à un seul objet, vous devez spécifier que le type d'autorisation est pour un objet. Pour ce faire, dans un appel d'API ou une commande CLI, transmettez le paramètre `s3PrefixType` avec la valeur `Object`. Dans la console Amazon S3, lorsque vous créez l'autorisation, après avoir sélectionné un emplacement, sous Portée de l'octroi, cochez la case Grant scope is an object (La portée de l'octroi est un objet).
> - Vous ne pouvez pas créer d'autorisation d'accès à un compartiment si celui-ci n'existe pas encore. Toutefois, vous pouvez créer une autorisation pour un préfixe qui n'existe pas encore.
> - Pour le nombre maximum d'autorisations d'accès que vous pouvez créer dans votre instance d'autorisations d'accès S3, consultez Limitations des autorisations d'accès S3.

Vous pouvez créer une autorisation d'accès à l'aide de la console Amazon S3 AWS CLI, de l'API REST Amazon S3 et AWS SDKs.

Utilisation de la console S3

Pour créer une autorisation d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.

   Si vous utilisez l'instance d'autorisations d'accès S3 pour la première fois, assurez-vous d'avoir terminé l'étape 2 : Enregistrer un emplacement et d'être passé à l'étape 3 de l'Assistant Mise en place de l'instance Access Grants. Si vous possédez déjà une instance d'autorisations d'accès S3, choisissez Afficher les détails, puis, dans l'onglet Octrois, choisissez Créer un octroi.

   a. Dans la section Portée de l'octroi, sélectionnez ou entrez un emplacement enregistré.

Si vous avez sélectionné l'emplacement `s3://` par défaut, utilisez la zone Sous-préfixe pour réduire la portée de l'autorisation d'accès. Pour plus d'informations, consultez Sous-préfixe. Si vous accordez l'accès uniquement à un objet, sélectionnez Le périmètre de l'octroi est un objet.

b. Sous Autorisations et accès, sélectionnez le niveau d'autorisation : Lecture, Écriture ou les deux.

   Choisissez ensuite le type de bénéficiaire. Si vous avez ajouté votre annuaire d'entreprise à IAM Identity Center et associé cette instance IAM Identity Center à votre instance d'autorisations d'accès S3, vous pouvez choisir Identité du répertoire depuis IAM Identity Center. Si vous choisissez cette option, obtenez l'ID de l'utilisateur ou du groupe auprès d'IAM Identity Center et entrez-le dans cette section.

   Si le type de bénéficiaire est un utilisateur ou un rôle IAM, choisissez Principal IAM. Sous Type principal d'IAM, choisissez Utilisateur ou Rôle. Ensuite, sous Utilisateur principal d'IAM, choisissez dans la liste ou entrez l'ID de l'identité.

c. Pour créer l'autorisation d'accès S3, choisissez Suivant ou Créer une autorisation.

4. Si l'option Suivant ou Créer un octroi est désactivée :

   Impossible de créer un octroi

   - Il se peut que vous deviez d'abord enregistrer un emplacement dans votre instance d'autorisations d'accès S3.
   - Vous ne disposez peut-être pas de l'autorisation `s3:CreateAccessGrant` pour créer une autorisation d'accès. Contactez l'administrateur de votre compte.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Les exemples suivants montrent comment créer une demande d'autorisation d'accès pour un principal IAM et comment créer une demande d'autorisation d'accès pour un utilisateur ou un groupe d'annuaire d'entreprise.

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

> **Note**
>
> Si vous créez une autorisation d'accès qui accorde l'accès à un seul objet, incluez le paramètre requis `--s3-prefix-type Object`.

Example Créer une demande d'autorisation d'accès pour un principal IAM

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
--access-grants-location-configuration S3SubPrefix=prefixB* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::123456789012:user/data-consumer-3
```

Example Créer une réponse d'octroi d'accès

```
{"CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/grant/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "AccessGrantsLocationId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
    "GrantScope": "s3://DOC-BUCKET-EXAMPLE/prefix*",
    "Permission": "READ"
}
```

Créer une demande d'autorisation d'accès pour un utilisateur ou un groupe d'annuaire

Pour créer une demande d'autorisation d'accès pour un utilisateur ou un groupe d'annuaire, vous devez d'abord obtenir le GUID de l'utilisateur ou du groupe d'annuaire en exécutant l'une des commandes suivantes.

Example Obtenir un GUID pour un utilisateur ou un groupe d'annuaire

Vous pouvez trouver le GUID d'un utilisateur IAM Identity Center via la console IAM Identity Center ou en utilisant le ou. AWS CLI AWS SDKs La commande suivante répertorie les utilisateurs de l'instance IAM Identity Center spécifiée, avec leurs noms et identifiants.

```
aws identitystore list-users --identity-store-id d-1a2b3c4d1234
```

Cette commande répertorie les groupes figurant dans l'instance IAM Identity Center spécifiée.

```
aws identitystore list-groups --identity-store-id d-1a2b3c4d1234
```

Example Créer une autorisation d'accès pour un utilisateur ou un groupe d'annuaire

Cette commande est similaire à la création d'un octroi pour des utilisateurs ou des rôles IAM, si ce n'est que le type de bénéficiaire est `DIRECTORY_USER` ou `DIRECTORY_GROUP`, et que l'identifiant du bénéficiaire est le GUID de l'utilisateur ou du groupe d'annuaire.

```
aws s3control create-access-grant \
--account-id 123456789012 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix="amzn-s3-demo-bucket/rafael/*" \
--permission READWRITE \
--grantee GranteeType=DIRECTORY_USER,GranteeIdentifier=83d43802-00b1-7054-db02-
f1d683aacba5 \
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la gestion des autorisations d'accès, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- CreateAccessGrant
- DeleteAccessGrant
- GetAccessGrant
- ListAccessGrants

En utilisant le AWS SDKs

Cette section fournit des exemples de création d'une autorisation d'accès à l'aide du AWS SDKs.

Java

Pour utiliser l'exemple suivant, remplacez les *user input placeholders* par vos propres informations :

> **Note**
>
> Si vous créez une autorisation d'accès qui accorde l'accès à un seul objet, incluez le paramètre requis `.s3PrefixType(S3PrefixType.Object)`.

Example Créer une demande d'autorisation d'accès

```
public void createAccessGrant() {
CreateAccessGrantRequest createRequest = CreateAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantsLocationId("a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa")
.permission("READ")
.accessGrantsLocationConfiguration(AccessGrantsLocationConfiguration.builder().s3SubPrefix("
.grantee(Grantee.builder().granteeType("IAM").granteeIdentifier("arn:aws:iam::111122223333:u
data-consumer-3").build())
.build();
CreateAccessGrantResponse createResponse =
 s3Control.createAccessGrant(createRequest);
LOGGER.info("CreateAccessGrantResponse: " + createResponse);
}
```

Example Créer une réponse d'octroi d'accès

```
CreateAccessGrantResponse(
CreatedAt=2023-06-07T05:20:26.330Z,
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
AccessGrantArn=arn:aws:s3:us-east-2:444455556666:access-grants/default/grant/
a1b2c3d4-5678-90ab-cdef-EXAMPLE33333,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
AccessGrantsLocationId=a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaaa,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
```

```
),
GrantScope=s3://DOC-BUCKET-EXAMPLE/prefixB,
Permission=READ
)
```

Affichage d'un octroi

Vous pouvez consulter les détails d'une autorisation d'accès dans votre instance Amazon S3 Access Grants en utilisant la console Amazon S3, le AWS Command Line Interface (AWS CLI), l'API REST Amazon S3 et le AWS SDKs.

Utilisation de la console S3

Pour afficher les détails d'une autorisation d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.
4. Choisissez Afficher les détails pour cette instance.
5. Sur la page des détails, choisissez l'onglet Octrois.
6. Dans la section Autorisations, recherchez l'autorisation d'accès que vous souhaitez consulter. Pour filtrer la liste des octrois, utilisez la zone de recherche.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser les exemples de commandes suivants, remplacez les *`user input placeholders`* par vos propres informations.

Example : Obtenir les détails d'une autorisation d'accès

```
aws s3control get-access-grant \
--account-id 111122223333 \
```

```
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

Réponse :

```
{
    "CreatedAt": "2023-05-31T18:41:34.663000+00:00",
    "AccessGrantId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Grantee": {
        "GranteeType": "IAM",
        "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
    },
    "Permission": "READ",
    "AccessGrantsLocationId": "12a6710f-5af8-41f5-b035-0bc795bf1a2b",
    "AccessGrantsLocationConfiguration": {
        "S3SubPrefix": "prefixB*"
    },
    "GrantScope": "s3://amzn-s3-demo-bucket/"
}
```

Example : Répertorier toutes les autorisations d'accès dans une instance d'autorisations d'accès S3

Vous pouvez éventuellement utiliser les paramètres suivants pour limiter les résultats à un préfixe S3 ou à une identité AWS Identity and Access Management (IAM) :

- Sous-préfixe : `--grant-scope s3://bucket-name/prefix*`
- Identité IAM : `--grantee-type IAM` et `--grantee-identifier arn:aws:iam::123456789000:role/accessGrantsConsumerRole`

```
aws s3control list-access-grants \
--account-id 111122223333
```

Réponse :

```
{
    "AccessGrantsList": [{"CreatedAt": "2023-06-14T17:54:46.542000+00:00",
            "AccessGrantId": "dd8dd089-b224-4d82-95f6-975b4185bbaa",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa",
```

```
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-3"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "23514a34-ea2e-4ddf-b425-d0d4bfcarda1",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixA*"
        },
        {"CreatedAt": "2023-06-24T17:54:46.542000+00:00",
            "AccessGrantId": "ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "AccessGrantArn": "arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2",
            "Grantee": {
                "GranteeType": "IAM",
                "GranteeIdentifier": "arn:aws:iam::111122223333:user/data-consumer-9"
            },
            "Permission": "READ",
            "AccessGrantsLocationId": "12414a34-ea2e-4ddf-b425-d0d4bfcacao0",
            "GrantScope": "s3://amzn-s3-demo-bucket/prefixB*"
        },

    ]
}
```

Utilisation de l'API REST

Vous pouvez utiliser les opérations d'API Amazon S3 pour consulter les détails d'une autorisation d'accès et répertorier toutes les autorisations d'accès dans une instance d'autorisations d'accès S3. Pour en savoir plus sur la prise en charge de l'API REST pour la gestion des autorisations d'accès, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- GetAccessGrant
- ListAccessGrants

En utilisant le AWS SDKs

Cette section fournit des exemples de la manière d'obtenir les détails d'une autorisation d'accès à l'aide du AWS SDKs.

Pour utiliser les exemples suivants, remplacez *`user input placeholders`* par vos propres informations.

Java

Example : Obtenir les détails d'un octroi d'accès

```
public void getAccessGrant() {
GetAccessGrantRequest getRequest = GetAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE22222")
.build();
GetAccessGrantResponse getResponse = s3Control.getAccessGrant(getRequest);
LOGGER.info("GetAccessGrantResponse: " + getResponse);
}
```

Réponse :

```
GetAccessGrantResponse(
CreatedAt=2023-06-07T05:20:26.330Z,
AccessGrantId=a1b2c3d4-5678-90ab-cdef-EXAMPLE22222,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant-fd3a5086-42f7-4b34-9fad-472e2942c70e,
Grantee=Grantee(
GranteeType=IAM,
GranteeIdentifier=arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=12a6710f-5af8-41f5-b035-0bc795bf1a2b,
AccessGrantsLocationConfiguration=AccessGrantsLocationConfiguration(
S3SubPrefix=prefixB*
),
GrantScope=s3://amzn-s3-demo-bucket/
)
```

Example : Répertorier tous les octrois d'accès dans une instance d'octrois d'accès S3

Vous pouvez éventuellement utiliser ces paramètres pour limiter les résultats à un préfixe S3 ou à une identité IAM :

- Portée : `GrantScope=s3://bucket-name/prefix*`
- Bénéficiaire : `GranteeType=IAM` et `GranteeIdentifier=arn:aws:iam::111122223333:role/accessGrantsConsumerRole`

```
public void listAccessGrants() {
ListAccessGrantsRequest listRequest = ListAccessGrantsRequest.builder()
.accountId("111122223333")
.build();
ListAccessGrantsResponse listResponse = s3Control.listAccessGrants(listRequest);
LOGGER.info("ListAccessGrantsResponse: " + listResponse);
}
```

Réponse :

```
ListAccessGrantsResponse(
AccessGrantsList=[
ListAccessGrantEntry(
CreatedAt=2023-06-14T17:54:46.540z,
AccessGrantId=dd8dd089-b224-4d82-95f6-975b4185bbaa,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/dd8dd089-b224-4d82-95f6-975b4185bbaa,
Grantee=Grantee(
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-3
),
Permission=READ,
AccessGrantsLocationId=23514a34-ea2e-4ddf-b425-d0d4bfcarda1,
GrantScope=s3://amzn-s3-demo-bucket/prefixA
),
ListAccessGrantEntry(
CreatedAt=2023-06-24T17:54:46.540Z,
AccessGrantId=ee8ee089-b224-4d72-85f6-975b4185a1b2,
AccessGrantArn=arn:aws:s3:us-east-2:111122223333:access-grants/default/
grant/ee8ee089-b224-4d72-85f6-975b4185a1b2,
Grantee=Grantee(
GranteeType=IAM, GranteeIdentifier= arn:aws:iam::111122223333:user/data-consumer-9
),
Permission=READ,
AccessGrantsLocationId=12414a34-ea2e-4ddf-b425-d0d4bfcacao0,
GrantScope=s3://amzn-s3-demo-bucket/prefixB*
)
]
)
```

Suppression d'un octroi

Vous pouvez supprimer des autorisations d'accès de votre instance d'autorisations d'accès Amazon S3. Vous ne pouvez pas annuler la suppression d'une autorisation d'accès. Une fois que vous avez supprimé une autorisation d'accès, le bénéficiaire n'a plus accès à vos données Amazon S3.

Vous pouvez supprimer une autorisation d'accès à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI), de l'API REST Amazon S3 et du AWS SDKs.

Utilisation de la console S3

Pour supprimer une autorisation d'accès

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Grants.
3. Sur la page Octrois d'accès S3, choisissez la région qui contient l'instance d'octrois d'accès S3 qui vous intéresse.
4. Choisissez Afficher les détails pour cette instance.
5. Sur la page des détails, choisissez l'onglet Octrois.
6. Recherchez l'octroi que vous souhaitez supprimer. Lorsque vous avez localisé l'octroi, choisissez la case d'option correspondante.
7. Sélectionnez Delete (Supprimer). Une boîte de dialogue apparaît pour vous avertir que cette action ne peut pas être annulée. Choisissez à nouveau Supprimer pour supprimer l'octroi.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Supprimer une autorisation d'accès

```
aws s3control delete-access-grant \
--account-id 111122223333 \
--access-grant-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

```
// No response body
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST Amazon S3 pour la gestion des autorisations d'accès, consultez DeleteAccessGrant dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS SDKs

Cette section fournit des exemples de suppression d'une autorisation d'accès à l'aide du AWS SDKs. Pour utiliser l'exemple suivant, remplacez les *`user input placeholders`* par vos propres informations.

Java

Example : Supprimer un octroi d'accès

```
public void deleteAccessGrant() {
DeleteAccessGrantRequest deleteRequest = DeleteAccessGrantRequest.builder()
.accountId("111122223333")
.accessGrantId("a1b2c3d4-5678-90ab-cdef-EXAMPLE11111")
.build();
DeleteAccessGrantResponse deleteResponse =
 s3Control.deleteAccessGrant(deleteRequest);
LOGGER.info("DeleteAccessGrantResponse: " + deleteResponse);
}
```

Réponse :

```
DeleteAccessGrantResponse()
```

Obtention de données S3 à l'aide d'autorisations d'accès

Les bénéficiaires qui ont obtenu l'accès aux données S3 via les autorisations d'accès S3 doivent demander des informations d'identification temporaires aux autorisations d'accès S3. Ils les utiliseront pour accéder aux données S3. Pour de plus amples informations, veuillez consulter Demande d'un accès aux données Amazon S3 via les autorisations d'accès S3. Les bénéficiaires utilisent ensuite ces informations d'identification temporaires pour effectuer des actions S3 autorisées sur les

données S3. Pour de plus amples informations, veuillez consulter Accès aux données S3 à l'aide des informations d'identification fournies par les autorisations d'accès S3. Les bénéficiaires peuvent éventuellement demander une liste de leurs autorisations d'accès pour et Compte AWS avant de demander ces informations d'identification. Pour de plus amples informations, veuillez consulter Répertorier les autorisations d'accès de l'appelant.

Rubriques

- Demande d'un accès aux données Amazon S3 via les autorisations d'accès S3
- Accès aux données S3 à l'aide des informations d'identification fournies par les autorisations d'accès S3
- Répertorier les autorisations d'accès de l'appelant

Demande d'un accès aux données Amazon S3 via les autorisations d'accès S3

Après avoir créé une autorisation d'accès à l'aide de S3 Access Grants, les bénéficiaires peuvent demander des informations d'identification pour accéder aux données S3 auxquelles ils ont été autorisés à accéder. Les bénéficiaires peuvent être des directeurs AWS Identity and Access Management (IAM), des identités de votre annuaire d'entreprise ou des applications autorisées.

Une application Service AWS peut utiliser l'opération d'`GetDataAccess`API S3 Access Grants pour demander à S3 Access Grants l'accès à vos données S3 au nom d'un bénéficiaire. `GetDataAccess`vérifie d'abord que vous avez accordé à cette identité l'accès aux données. Les autorisations d'accès S3 utilisent l'opération d'API AssumeRole pour obtenir un jeton d'informations d'identification temporaire et le transmettent au demandeur. Ce jeton d'informations d'identification temporaire est un jeton AWS Security Token Service (AWS STS).

La demande `GetDataAccess` doit inclure le paramètre `target`, qui spécifie la portée des données S3 à laquelle s'appliquent les informations d'identification temporaires. Cette `target` portée peut être identique à celle de la subvention ou à un sous-ensemble de cette portée, mais elle doit être comprise dans le cadre de la subvention accordée au bénéficiaire. `target` La demande doit également spécifier le paramètre `permission` pour indiquer le niveau d'autorisation pour les informations d'identification temporaires, que ce soit `READ`, `WRITE` ou `READWRITE`.

Privilège

Le demandeur peut spécifier le niveau de privilège du jeton temporaire dans sa demande d'informations d'identification. À l'aide du paramètre `privilege`, le demandeur peut réduire ou augmenter la portée d'accès des informations d'identification temporaires, dans les limites de la

portée de l'octroi. La valeur par défaut du paramètre `privilege` est `Default`, ce qui signifie que la portée cible des informations d'identification renvoyées est la portée de l'octroi d'origine. L'autre valeur possible pour `privilege` est `Minimal`. Si la portée `target` est réduite par rapport à la portée de l'octroi d'origine, la portée des informations d'identification temporaires est désactivée pour correspondre à la portée `target`, à condition que la portée `target` soit comprise dans la portée de l'octroi.

Le tableau suivant détaille l'effet du paramètre `privilege` sur deux octrois. Un octroi a la portée `S3://amzn-s3-demo-bucket1/bob/*`, qui inclut l'intégralité du préfixe `bob/` dans le compartiment *amzn-s3-demo-bucket1*. L'autre octroi a la portée `S3://amzn-s3-demo-bucket1/bob/reports/*`, qui inclut uniquement le préfixe `bob/reports/` dans le compartiment *amzn-s3-demo-bucket1*.

Portée de l'octroi	Portée demandée	Privilège	Portée renvoyée	Effet
S3://*amzn-s3-demo-bucket1* /bob/*	*amzn-s3-demo-bucket1* /bob/*	Default	*amzn-s3-demo-bucket1* /bob/*	Le demandeur a accès à tous les objets qui ont des noms de clé commençant par le préfixe *bob/* dans le compartiment *amzn-s3-demo-bucket1* .
S3://*amzn-s3-demo-bucket1* /bob/*	*amzn-s3-demo-bucket1* /bob/	Minimal	*amzn-s3-demo-bucket1* /bob/	Sans le caractère générique * après le nom de préfixe bob/, le demandeur n'a accès qu'à l'objet nommé bob/ dans le compartiment *amzn-s3-demo-bucket1* . Il n'est pas courant d'avoir un tel objet. Le demandeur n'a accès à aucun autre objet, pas même à ceux ayant des noms de clé commençant par le préfixe bob/.

Portée de l'octroi	Portée demandée	Privilège	Portée renvoyée	Effet
S3://*amzn-s3-demo-bucket1* /bob/*	*amzn-s3-demo-bucket1* /bob/images/*	Minimal	*amzn-s3-demo-bucket1* /bob/images/*	Le demandeur a accès à tous les objets qui ont des noms de clé commençant par le préfixe *bob/images/** dans le compartiment *amzn-s3-demo-bucket1* .
S3://*amzn-s3-demo-bucket1* /bob/reports/*	*amzn-s3-demo-bucket1* /bob/reports/file.txt	Default	*amzn-s3-demo-bucket1* /bob/reports/*	Le demandeur a accès à tous les objets qui ont des noms de clé commençant par le préfixe bob/reports dans le compartiment *amzn-s3-demo-bucket1* , ce qui correspond à la portée de l'octroi correspondant.
S3://*amzn-s3-demo-bucket1* /bob/reports/*	*amzn-s3-demo-bucket1* /bob/reports/file.txt	Minimal	*amzn-s3-demo-bucket1* /bob/reports/file.txt	Le demandeur a accès uniquement à l'objet doté du nom de clé bob/reports/file.txt dans le compartiment *amzn-s3-demo-bucket1* . Le demandeur n'a accès à aucun autre objet.

Identités des annuaires

GetDataAccessprend en compte toutes les identités impliquées dans une demande lorsqu'il s'agit de jumeler des subventions appropriées. Pour les identités d'annuaire d'entreprise, renvoie GetDataAccess également les autorisations de l'identité IAM utilisée pour la session basée

sur l'identité. Pour plus d'informations sur les sessions basées sur l'identité, consultez la section Octroi d'autorisations pour utiliser des sessions de console basées sur l'identité dans le Guide de l'utilisateur.AWS Identity and Access Management `GetDataAccess`génère des informations d'identification limitant la portée à l'autorisation la plus restrictive, comme indiqué dans le tableau suivant :

Champ d'application de la subvention pour l'identité IAM	Octroi d'une portée pour l'identité du répertoire	Portée demandée	Portée renvoyée	Privilège	Effet
S3://*amzn-s3-demo-bucket1* / bob/*	*amzn-s3-demo-bucket1* / bob/images/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/*	Default	Le demandeur a accès à tous les objets dont les noms de clé commencent par le préfixe bob/ dans le cadre de l'attribution du rôle IAM, mais il est limité aux préfixes bob/images/ dans le cadre de l'attribution de l'identité du répertoire. Le rôle IAM et l'identité de répertoire fournissent tous deux l'accès à l'étendue demandéebob/images/image1.jpeg , mais l'identité de répertoire bénéficie d'une autorisation plus restrictive. La portée renvoyée est

Champ d'application de la subvention pour l'identité IAM	Octroi d'une portée pour l'identité du répertoire	Portée demandée	Portée renvoyée	Privilège	Effet
					donc limitée à l'attribution la plus restrictive de l'identité du répertoire.
S3://*amzn-s3-demo-bucket1* / bob/*	*amzn-s3-demo-bucket1* / bob/images/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	`Minimal`	Étant donné que le privilège est défini sur`Minimal`, même si l'identité a accès à une plus grande étendue, seule l'étendue demandée est renvoyée`bob/images/image1.jpeg` .

Champ d'application de la subvention pour l'identité IAM	Octroi d'une portée pour l'identité du répertoire	Portée demandée	Portée renvoyée	Privilège	Effet
S3://*amzn-s3-demo-bucket1* / bob/images/*	*amzn-s3-demo-bucket1* / bob/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/*	Default	Le demandeur a accès à tous les objets dont les noms de clé commencent par le préfixe bob/ dans le cadre de l'attribution de l'identité du répertoire, mais il est limité aux préfixes bob/images/ dans le cadre de l'attribution du rôle IAM. Le rôle IAM et l'identité de répertoire fournissent tous deux l'accès à l'étendue demandéebob/images/image1.jpeg , mais le rôle IAM dispose d'une autorisation plus restrictive. La portée renvoyée est donc limitée à l'attribution la plus restrictive pour le rôle IAM.

Champ d'application de la subvention pour l'identité IAM	Octroi d'une portée pour l'identité du répertoire	Portée demandée	Portée renvoyée	Privilège	Effet
S3://*amzn-s3-demo-bucket1* / bob/images/*	*amzn-s3-demo-bucket1* / bob/*	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	S3://*amzn-s3-demo-bucket1* / bob/images/image1.jpeg	Minimal	Étant donné que le privilège est défini surMinimal, même si l'identité a accès à une plus grande étendue, seule l'étendue demandée est renvoyéebob/images/image1.jpeg .

Durée

Le paramètre durationSeconds définit la durée des informations d'identification temporaires, en secondes. La valeur par défaut est de 3600 secondes (1 heure), mais le demandeur (le bénéficiaire) peut spécifier une plage allant de 900 secondes (15 minutes) à 43200 secondes (12 heures). Si le bénéficiaire demande une valeur supérieure à ce maximum, la demande échoue.

> **Note**
>
> Dans votre demande de jeton temporaire, si l'emplacement est un objet, définissez la valeur du paramètre targetType dans votre demande sur Object. Ce paramètre est obligatoire seulement si l'emplacement est un objet et que le niveau de privilège est Minimal. Si l'emplacement est un compartiment ou un préfixe, vous n'avez pas besoin de spécifier ce paramètre.

Exemples

Vous pouvez demander des informations d'identification temporaires en utilisant le AWS Command Line Interface (AWS CLI), l'API REST Amazon S3 et le AWS SDKs. Veuillez consulter ces exemples.

Pour plus d'informations, consultez GetDataAccessle manuel Amazon Simple Storage Service API Reference.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example Demander des informations d'identification temporaires

Requête :

```
aws s3control get-data-access \
--account-id 111122223333 \
--target s3://amzn-s3-demo-bucket/prefixA* \
--permission READ \
--privilege Default \
--region us-east-2
```

Réponse :

```
{
"Credentials": {
"AccessKeyId": "Example-key-id",
"SecretAccessKey": "Example-access-key",
"SessionToken": "Example-session-token",
"Expiration": "2023-06-14T18:56:45+00:00"},
"MatchedGrantTarget": "s3://amzn-s3-demo-bucket/prefixA**",
"Grantee": {
    "GranteeType": "IAM",
    "GranteeIdentifier": "arn:aws:iam::111122223333:role/role-name"
 }
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge par l'API REST d'Amazon S3 pour la demande d'informations d'identification temporaires auprès de S3 Access Grants, consultez GetDataAccessle manuel Amazon Simple Storage Service API Reference.

En utilisant le AWS SDKs

Cette section fournit un exemple de la façon dont les bénéficiaires demandent des informations d'identification temporaires à S3 Access Grants en utilisant le AWS SDKs.

Java

L'exemple de code suivant renvoie les informations d'identification temporaires que le bénéficiaire utilise pour accéder à vos données S3. Pour utiliser cet exemple de code, remplacez les *`user input placeholders`* par vos propres informations.

Example Obtenir des informations d'identification temporaires

Requête :

```
public void getDataAccess() {
GetDataAccessRequest getDataAccessRequest = GetDataAccessRequest.builder()
.accountId("111122223333")
.permission(Permission.READ)
.privilege(Privilege.MINIMAL)
.target("s3://amzn-s3-demo-bucket/prefixA*")
.build();
GetDataAccessResponse getDataAccessResponse =
 s3Control.getDataAccess(getDataAccessRequest);
LOGGER.info("GetDataAccessResponse: " + getDataAccessResponse);
}
```

Réponse :

```
GetDataAccessResponse(
Credentials=Credentials(
AccessKeyId="Example-access-key-id",
SecretAccessKey="Example-secret-access-key",
SessionToken="Example-session-token",
Expiration=2023-06-07T06:55:24Z
))
```

Accès aux données S3 à l'aide des informations d'identification fournies par les autorisations d'accès S3

Une fois qu'un bénéficiaire a obtenu des informations d'identification temporaires via son autorisation d'accès, il peut utiliser ces informations d'identification temporaires pour appeler les opérations d'API Amazon S3 afin d'accéder à vos données.

Les bénéficiaires peuvent accéder aux données S3 en utilisant le AWS Command Line Interface (AWS CLI) AWS SDKs, le et l'API REST Amazon S3. En outre, vous pouvez utiliser les plugins AWS Python et Java pour appeler S3 Access Grants

En utilisant le AWS CLI

Une fois que le bénéficiaire a obtenu ses informations d'identification temporaires auprès des autorisations d'accès S3, il peut configurer un profil avec ces informations d'identification pour récupérer les données.

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser les exemples de commandes suivants, remplacez les *user input placeholders* par vos propres informations.

Example : Configurer un profil

```
aws configure set aws_access_key_id "$accessKey" --profile access-grants-consumer-access-profile
aws configure set aws_secret_access_key "$secretKey" --profile access-grants-consumer-access-profile
aws configure set aws_session_token "$sessionToken" --profile access-grants-consumer-access-profile
```

Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example : Obtenir les données S3

Le bénéficiaire peut utiliser la get-object AWS CLI commande pour accéder aux données. Le bénéficiaire peut également utiliser put-objectls, et d'autres AWS CLI commandes S3.

```
aws s3api get-object \
```

```
--bucket amzn-s3-demo-bucket1 \
--key myprefix \
--region us-east-2 \
--profile access-grants-consumer-access-profile
```

En utilisant le AWS SDKs

Cette section fournit des exemples de la manière dont les bénéficiaires peuvent accéder à vos données S3 à l'aide du AWS SDKs.

Java

Pour des exemples expliquant comment obtenir des données S3 à l'aide d'informations d'identification temporaires, découvrez comment obtenir un objet à l'aide des exemples de code AWS SDKs et Amazon S3 pour le AWS SDK for Java 2.x.

Actions S3 prises en charge dans les autorisations d'accès S3

Un bénéficiaire peut utiliser les informations d'identification temporaires fournies par les autorisations d'accès S3 pour effectuer des actions S3 sur les données S3 auxquelles il a accès. Voici une liste des actions S3 qui peuvent être autorisées et qu'un bénéficiaire peut effectuer. Les actions qui peuvent être autorisées dépendent du niveau d'autorisation accordé dans l'autorisation d'accès : `READ`, `WRITE` ou `READWRITE`.

> **Note**
>
> Outre les autorisations Amazon S3 répertoriées ci-dessous, Amazon S3 peut appeler l'autorisation AWS Key Management Service (AWS KMS) Decrypt (`kms:decrypt`) ou l'`READ`autorisation AWS KMS GenerateDataKey(`kms:generateDataKey`)`WRITE`. Ces autorisations ne permettent pas d'accéder directement à la AWS KMS clé.

Action IAM S3	Action d'API et documentation	Autorisation d'octroi d'accès S3	Ressource S3			
`s3:GetObject`	GetObject	`READ`	Objet			

Action IAM S3	Action d'API et documentation	Autorisation d'octroi d'accès S3	Ressource S3			
`s3:GetObjectVersion`	GetObject	`READ`	Objet			
`s3:GetObjectAcl`	GetObjectAcl	`READ`	Objet			
`s3:GetObjectVersionAcl`	GetObjectAcl	`READ`	Objet			
`s3:ListMultipartUploads`	ListParts	`READ`	Objet			
`s3:PutObject`	PutObject, CreateMultipartUpload, UploadPart, UploadPartCopy, CompleteMultipartUpload	`WRITE`	Objet			
`s3:PutObjectAcl`	PutObjectAcl	`WRITE`	Objet			
`s3:PutObjectVersionAcl`	PutObjectAcl	`WRITE`	Objet			
`s3:DeleteObject`	DeleteObject	`WRITE`	Objet			

Action IAM S3	Action d'API et documentation	Autorisation d'octroi d'accès S3	Ressource S3			
`s3:DeleteObjectVersion`	DeleteObject	`WRITE`	Objet			
`s3:AbortMultipartUpload`	AbortMultipartUpload	`WRITE`	Objet			
`s3:ListBucket`	HeadBucket, ListObjectsV2, ListObjects	`READ`	Compartiment			
`s3:ListBucketVersions`	ListObjectVersions	`READ`	Compartiment			
`s3:ListBucketMultipartUploads`	ListMultipartUploads	`READ`	Compartiment			

Répertorier les autorisations d'accès de l'appelant

Les propriétaires de données S3 peuvent utiliser les subventions d'accès S3 pour créer des autorisations d'accès pour les identités AWS Identity and Access Management (IAM) ou pour les identités AWS IAM Identity Center d'annuaires d'entreprise. Les identités IAM et les identités d'annuaire IAM Identity Center peuvent à leur tour utiliser l'API `ListCallerAccessGrants` pour répertorier tous les compartiments, préfixes et objets Amazon S3 auxquels elles peuvent accéder, tels que définis par leurs autorisations d'accès S3. Utilisez cette API pour découvrir toutes les données S3 auxquelles une identité IAM ou une identité d'annuaire peut accéder via les autorisations d'accès S3.

Vous pouvez utiliser cette fonctionnalité pour créer des applications qui affichent les données accessibles à des utilisateurs finaux spécifiques. Par exemple, le navigateur de AWS stockage

pour S3, un composant d'interface utilisateur open source que les clients utilisent pour accéder aux compartiments S3, utilise cette fonctionnalité pour présenter aux utilisateurs finaux les données auxquelles ils ont accès dans Amazon S3, en fonction de leurs autorisations d'accès S3. Autre exemple : lorsque vous créez une application pour parcourir, charger ou télécharger des données dans Amazon S3, vous pouvez utiliser cette fonctionnalité pour créer une arborescence dans votre application qu'un utilisateur final pourra ensuite parcourir.

> **Note**
>
> Pour les identités d'annuaire d'entreprise, lors de la liste des autorisations d'accès de l'appelant, S3 Access Grants renvoie les autorisations de l'identité IAM utilisée pour la session basée sur l'identité. Pour plus d'informations sur les sessions basées sur l'identité, consultez la section Octroi d'autorisations pour utiliser des sessions de console basées sur l'identité dans le Guide de l'utilisateur.AWS Identity and Access Management

Le bénéficiaire, qu'il s'agisse d'une identité IAM ou d'une identité d'annuaire d'entreprise, peut obtenir la liste de ses autorisations d'accès en utilisant le AWS Command Line Interface (AWS CLI), l'API REST Amazon S3 et le. AWS SDKs

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Pour utiliser l'exemple de commande suivant, remplacez les *`user input placeholders`* par vos propres informations.

Example Affichage des autorisations d'accès accordées à un appelant

Requête :

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--max-results 5
```

Réponse :

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix1/*",
   "ApplicationArn": "NA"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix2/*",
   "ApplicationArn": "ALL"
  },
  {
   "Permission": "READWRITE",
   "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/sub-prefix3/*",
   "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
  }
 ]
}
```

Example Répertorier les autorisations d'accès d'un appelant pour un compartiment

Vous pouvez limiter la portée des résultats à l'aide du paramètre `grantscope`.

Requête :

```
aws s3control list-caller-access-grants \
--account-id 111122223333 \
--region us-east-2
--grant-scope "s3://amzn-s3-demo-bucket""
--max-results 1000
```

Réponse :

```
{
 "NextToken": "6J9S...",
 "CallerAccessGrantsList": [
  {
   "Permission": "READ",
```

```
    "GrantScope": "s3://amzn-s3-demo-bucket*",
    "ApplicationArn": "ALL"
   },
   {
    "Permission": "READ",
    "GrantScope": "s3://amzn-s3-demo-bucket/prefix1/*",
    "ApplicationArn": "arn:aws:sso::111122223333:application/ssoins-
ssoins-1234567890abcdef/apl-abcd1234a1b2c3d"
   }
 ]
}
```

Utilisation de l'API REST

Pour plus d'informations sur la prise en charge de l'API REST d'Amazon S3 pour obtenir une liste des autorisations d'accès accordées à l'appelant ListCallerAccessGrantsà l'API, consultez le manuel Amazon Simple Storage Service API Reference.

En utilisant le AWS SDKs

Cette section fournit un exemple de la façon dont les bénéficiaires demandent des informations d'identification temporaires à S3 Access Grants en utilisant le AWS SDKs.

Java

L'exemple de code suivant renvoie les autorisations d'accès de l'appelant de l'API aux données S3 d'un utilisateur donné Compte AWS. Pour utiliser cet exemple de code, remplacez les *user input placeholders* par vos propres informations.

Example Affichage des autorisations d'accès accordées à un appelant

Requête :

```
Public void ListCallerAccessGrants() {
 ListCallerAccessGrantsRequest listRequest = ListCallerAccessGrantsRequest.builder()
    .withMaxResults(1000)
    .withGrantScope("s3://")
    .accountId("111122223333");
 ListCallerAccessGrantsResponse listResponse =
 s3control.listCallerAccessGrants(listRequest);
 LOGGER.info("ListCallerAccessGrantsResponse: " + listResponse);
 }
```

Réponse :

```
ListCallerAccessGrantsResponse(
CallerAccessGrantsList=[
 ListCallerAccessGrantsEntry(
  S3Prefix=s3://amzn-s3-demo-bucket/prefix1/,
  Permission=READ,
  ApplicationArn=ALL
 )
])
```

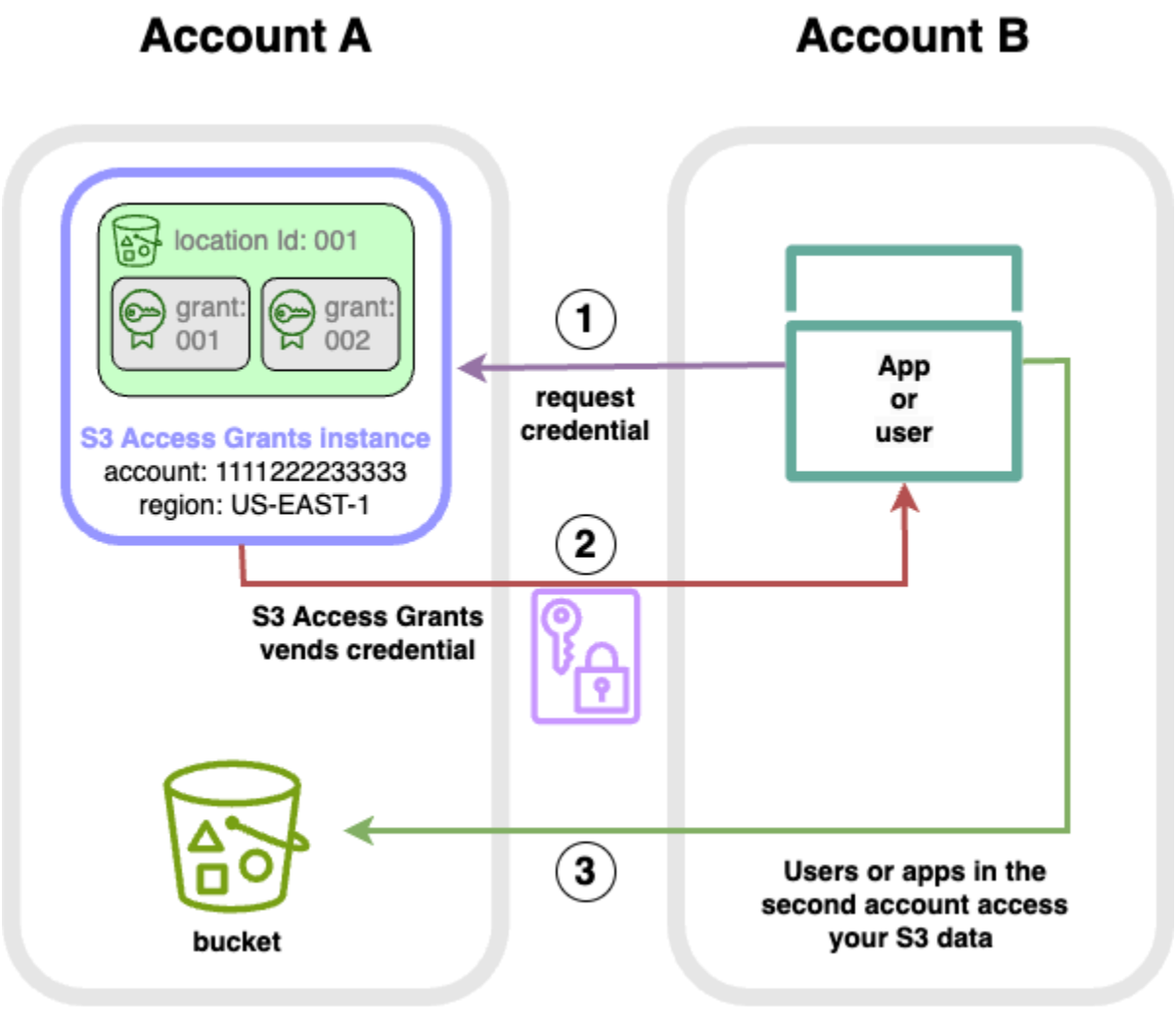
Accès intercompte aux autorisations d'accès S3

Avec les autorisations d'accès S3, vous pouvez accorder l'accès aux données Amazon S3 aux éléments suivants :

- AWS Identity and Access Management identités (IAM) au sein de votre compte
- Identités IAM dans d'autres comptes AWS
- Répertoriez les utilisateurs ou les groupes de votre AWS IAM Identity Center instance

Configurez d'abord l'accès intercompte pour l'autre compte. Cela inclut l'octroi de l'accès à votre instance d'autorisations d'accès S3 à l'aide d'une politique de ressources. Accordez ensuite l'accès à vos données S3 (compartiments, préfixes ou objets) en utilisant des autorisations.

Après avoir configuré l'accès intercompte, l'autre compte peut demander des informations d'accès temporaires à vos données Amazon S3 auprès des autorisations d'accès S3. L'image suivante montre le flux d'utilisateurs pour l'accès intercompte S3 via les autorisations d'accès S3 :



1. Les utilisateurs ou les applications d'un deuxième compte (B) demandent des informations d'identification à l'instance d'autorisations d'accès S3 de votre compte (A), où les données Amazon S3 sont stockées. Pour de plus amples informations, veuillez consulter Demande d'un accès aux données Amazon S3 via les autorisations d'accès S3.
2. L'instance d'autorisations d'accès S3 de votre compte (A) renvoie des informations d'identification temporaires si une autorisation permet au deuxième compte d'accéder à vos données Amazon S3. Pour plus d'informations sur les autorisations d'accès, consultez Octroi d'autorisations avec les autorisations d'accès S3.
3. Les utilisateurs ou les applications du second compte (B) utilisent les informations d'identification fournies par les autorisations d'accès S3 pour accéder aux données S3 de votre compte (A).

Configuration de l'accès intercompte avec les autorisations d'accès S3

Pour accorder un accès S3 intercompte via les autorisations d'accès S3, procédez comme suit :

- Étape 1 : configurez une instance d'autorisations d'accès S3 dans votre compte (par exemple, l'ID de compte 111122223333), où les données S3 sont stockées.
- Étape 2 : configurez la politique de ressources pour l'instance d'autorisations d'accès S3 de votre compte 111122223333 afin de donner accès au deuxième compte (par exemple, l'ID de compte 444455556666).
- Étape 3 : configurez les autorisations IAM pour que le principal IAM du deuxième compte 444455556666 demande des informations d'identification à l'instance d'autorisations d'accès S3 de votre compte 111122223333.
- Étape 4 : créez une autorisation dans votre compte 111122223333 qui donne au principal IAM du deuxième compte 444455556666 l'accès à certaines des données S3 de votre compte 111122223333.

Étape 1 : configurer une instance d'autorisations d'accès S3 dans votre compte

Tout d'abord, vous devez disposer d'une instance d'autorisations d'autorisations d'accès S3 dans votre compte 111122223333 pour gérer l'accès à vos données Amazon S3. Vous devez créer une instance d'autorisations d'accès S3 dans chaque Région AWS où sont stockées les données S3 que vous souhaitez partager. Si vous partagez des données dans plusieurs unités Région AWS, répétez chacune de ces étapes de configuration pour chacune d'entre elles Région AWS. Si vous disposez déjà d'une instance S3 Access Grants dans l' Région AWS endroit où sont stockées vos données S3, passez à l'étape suivante. Si vous n'avez pas configuré d'instance d'autorisations d'accès S3, consultez Utilisation des instances d'autorisations d'accès S3 pour mener à bien cette étape.

Étape 2 : configurer la politique de ressource pour votre instance d'autorisations d'accès S3 afin d'accorder un accès intercompte

Après avoir créé une instance d'autorisations d'accès S3 dans votre compte 111122223333 pour un accès intercompte, configurez la politique basée sur les ressources pour l'instance d'autorisations d'accès S3 de votre compte 111122223333 afin d'accorder un accès intercompte. L'instance d'autorisations d'accès S3 elle-même prend en charge les politiques basées sur les ressources. Lorsque la bonne politique basée sur les ressources est en place, vous pouvez accorder l'accès à des utilisateurs AWS Identity and Access Management (IAM) ou à des rôles provenant d'autres utilisateurs Comptes AWS à votre instance S3 Access Grants. L'accès intercompte accorde uniquement ces autorisations (actions) :

- `s3:GetAccessGrantsInstanceForPrefix` : l'utilisateur, le rôle ou l'application peut récupérer l'instance d'autorisations d'accès S3 qui contient un préfixe particulier.
- `s3:ListAccessGrants`
- `s3:ListAccessLocations`
- `s3:ListCallerAccessGrants`
- `s3:GetDataAccess` : l'utilisateur, le rôle ou l'application peut demander des informations d'identification temporaires en fonction de l'accès qui vous a été accordé via les autorisations d'accès S3. Utilisez ces informations d'identification pour accéder aux données S3 auxquelles l'accès vous a été accordé.

Parmi ces autorisations, vous pouvez choisir les autorisations à inclure dans la politique de ressources. Cette politique de ressources sur l'instance d'autorisations d'accès S3 est une politique standard basée sur les ressources et prend en charge tout ce que le langage de politique IAM prend en charge. Dans la même politique, vous pouvez accorder l'accès à des identités IAM spécifiques dans le compte `111122223333` (par exemple, avec la condition `aws:PrincipalArn`), mais vous n'êtes pas obligé de le faire avec les autorisations d'accès S3. À la place, au sein de votre instance d'autorisations d'accès S3, vous pouvez créer des autorisations pour des identités IAM individuelles à partir de votre compte, ainsi que pour l'autre compte. En gérant chaque autorisation d'accès via les autorisations d'accès S3, vous pouvez mettre à l'échelle vos autorisations.

Si vous utilisez déjà AWS Resource Access Manager (AWS RAM), vous pouvez y recourir pour partager vos ressources `s3:AccessGrants` avec d'autres comptes ou au sein de votre organisation. Consultez la section Utilisation de AWS ressources partagées pour plus d'informations. Si vous ne l'utilisez pas AWS RAM, vous pouvez également ajouter la politique de ressources en utilisant les opérations de l'API S3 Access Grants ou le AWS Command Line Interface (AWS CLI).

Utilisation de la console S3

Nous vous recommandons d'utiliser la console AWS Resource Access Manager (AWS RAM) pour partager vos `s3:AccessGrants` ressources avec d'autres comptes ou au sein de votre organisation. Pour partager les autorisations d'accès S3 intercompte, procédez comme suit :

Pour configurer la politique de ressources de l'instance d'autorisations d'accès S3 :

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Sélectionnez-le dans Région AWS le Région AWS sélecteur.

3. Dans le volet de navigation de gauche, sélectionnez Access Grants.
4. Sur la page de l'instance d'autorisations d'accès, dans la section Instance dans ce compte, sélectionnez Partager une instance. Cela vous redirigera vers la AWS RAM console.
5. Sélectionnez Créer un partage de ressources.
6. Suivez les AWS RAM étapes pour créer le partage de ressources. Pour plus d'informations, consultez la section Création d'un partage de ressources dans AWS RAM.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Vous pouvez ajouter la politique de ressources à l'aide de la commande CLI `put-access-grants-instance-resource-policy`.

Si vous souhaitez accorder un accès intercompte pour l'instance d'autorisations d'accès S3 se trouvant dans votre compte `111122223333` au deuxième compte `444455556666`, la politique de ressources de l'instance d'autorisations d'accès S3 de votre compte `111122223333` doit autoriser le deuxième compte `444455556666` à effectuer les actions suivantes :

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Dans la politique de ressources de l'instance d'autorisations d'accès S3, spécifiez l'ARN de votre instance d'autorisations d'accès S3 comme `Resource`, et le deuxième compte `444455556666` comme `Principal`. Pour utiliser l'exemple suivant, remplacez les *`user input placeholders`* par vos propres informations.

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
```

```
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

Pour ajouter ou mettre à jour une politique de ressources pour une instance d'autorisations d'accès S3, utilisez la commande suivante. Lorsque vous utilisez l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

Example Ajout ou mise à jour de la politique de ressources pour une instance d'autorisations d'accès S3

```
aws s3control put-access-grants-instance-resource-policy \
--account-id 111122223333 \
--policy file://resourcePolicy.json \
--region us-east-2
{
 "Policy": "{\n
   \"Version\": \"2012-10-17\",\n
   \"Statement\": [{\n
  \"Effect\": \"Allow\",\n
  \"Principal\": {\n
    \"AWS\": \"444455556666\"\n
  },\n
  \"Action\": [\n
    \"s3:ListAccessGrants\",\n
    \"s3:ListAccessGrantsLocations\",\n
    \"s3:GetDataAccess\",\n
    \"s3:GetAccessGrantsInstanceForPrefix\",\n
    \"s3:ListCallerAccessGrants\"\n
  ],\n
  \"Resource\": \"arn:aws:s3:us-east-2:111122223333:access-grants/default\"\n
    }\n
   ]\n
   }\n",
 "CreatedAt": "2023-06-16T00:07:47.473000+00:00"
```

```
}
```

Example Obtenir une politique de ressources d'autorisations d'accès S3

Vous pouvez également utiliser l'interface de ligne de commande pour obtenir ou supprimer une politique de ressources pour une instance d'autorisations d'accès S3.

Pour obtenir une politique de ressources d'autorisations d'accès S3, utilisez l'exemple de commande suivant. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-access-grants-instance-resource-policy \
--account-id 111122223333 \
--region us-east-2

{
"Policy": "{\"Version\":\"2012-10-17\",\"Statement\":[{\"Effect\":\"Allow
\",\"Principal\":{\"AWS\":\"arn:aws:iam::111122223333:root\"},\"Action\":
[\"s3:ListAccessGrants\",\"s3:ListAccessGrantsLocations\",\"s3:GetDataAccess\",
\"s3:GetAccessGrantsInstanceForPrefix\",\"s3:ListCallerAccessGrants\"],\"Resource\":
\"arn:aws:
s3:us-east-2:111122223333:access-grants/default\"}]}",
"CreatedAt": "2023-06-16T00:07:47.473000+00:00"
}
```

Example Supprimer une politique de ressources d'autorisations d'accès S3

Pour supprimer une politique de ressources d'autorisations d'accès S3, utilisez l'exemple de commande suivant. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control delete-access-grants-instance-resource-policy \
--account-id 111122223333 \
--region us-east-2

// No response body
```

Utilisation de l'API REST

Vous pouvez ajouter la politique de ressources à l'aide de l'PutAccessGrantsInstanceResourcePolicy API.

Si vous souhaitez accorder un accès intercompte pour l'instance d'autorisations d'accès S3 se trouvant dans votre compte 111122223333 au deuxième compte 444455556666, la politique de ressources de l'instance d'autorisations d'accès S3 de votre compte 111122223333 doit autoriser le deuxième compte 444455556666 à effectuer les actions suivantes :

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Dans la politique de ressources de l'instance d'autorisations d'accès S3, spécifiez l'ARN de votre instance d'autorisations d'accès S3 comme `Resource`, et le deuxième compte 444455556666 comme `Principal`. Pour utiliser l'exemple suivant, remplacez les *`user input placeholders`* par vos propres informations.

```
{
"Version": "2012-10-17",
"Statement": [
{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

Vous pouvez ensuite utiliser l'PutAccessGrantsInstanceResourcePolicy API pour configurer la politique.

Pour plus d'informations sur la prise en charge de l'API REST pour mettre à jour, obtenir ou supprimer une instance d'autorisations d'accès S3, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- PutAccessGrantsInstanceResourcePolicy
- GetAccessGrantsInstanceResourcePolicy
- DeleteAccessGrantsInstanceResourcePolicy

En utilisant le AWS SDKs

Cette section fournit des exemples du AWS SDK expliquant comment configurer votre politique de ressources S3 Access Grants afin d'accorder à un deuxième AWS compte l'accès à certaines de vos données S3.

Java

Ajoutez, mettez à jour, obtenez ou supprimez une politique de ressources pour gérer l'accès intercompte à votre instance d'autorisations d'accès S3.

Example Ajout ou mise à jour d'une politique de ressources pour une instance d'autorisations d'accès S3

Si vous souhaitez accorder un accès intercompte pour l'instance d'autorisations d'accès S3 se trouvant dans votre compte `111122223333` au deuxième compte `444455556666`, la politique de ressources de l'instance d'autorisations d'accès S3 de votre compte `111122223333` doit autoriser le deuxième compte `444455556666` à effectuer les actions suivantes :

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`

Dans la politique de ressources de l'instance d'autorisations d'accès S3, spécifiez l'ARN de votre instance d'autorisations d'accès S3 comme `Resource`, et le deuxième compte `444455556666` comme `Principal`. Pour utiliser l'exemple suivant, remplacez les *`user input placeholders`* par vos propres informations.

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

```
 "Principal": {
 "AWS": "444455556666"
},
 "Action": [
  "s3:ListAccessGrants",
  "s3:ListAccessGrantsLocations",
  "s3:GetDataAccess",
  "s3:GetAccessGrantsInstanceForPrefix"
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
} ]
}
```

Pour ajouter ou mettre à jour la politique de ressources d'une instance d'autorisations d'accès S3, utilisez l'exemple de code suivant :

```
public void putAccessGrantsInstanceResourcePolicy() {
 PutAccessGrantsInstanceResourcePolicyRequest putRequest =
 PutAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .policy(RESOURCE_POLICY)
 .build();
 PutAccessGrantsInstanceResourcePolicyResponse putResponse =
 s3Control.putAccessGrantsInstanceResourcePolicy(putRequest);
 LOGGER.info("PutAccessGrantsInstanceResourcePolicyResponse: " + putResponse);
 }
```

Réponse :

```
PutAccessGrantsInstanceResourcePolicyResponse(
 Policy={
 "Version": "2012-10-17",
 "Statement": [{
 "Effect": "Allow",
 "Principal": {
 "AWS": "444455556666"
 },
 "Action": [
 "s3:ListAccessGrants",
 "s3:ListAccessGrantsLocations",
 "s3:GetDataAccess",
 "s3:GetAccessGrantsInstanceForPrefix",
 "s3:ListCallerAccessGrants"
```

```
 ],
 "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
 }]
 }
 )
```

Example Obtenir une politique de ressources d'autorisations d'accès S3

Pour obtenir une politique de ressources d'autorisations d'accès S3, utilisez l'exemple de code suivant. Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

```
public void getAccessGrantsInstanceResourcePolicy() {
 GetAccessGrantsInstanceResourcePolicyRequest getRequest =
 GetAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
 .build();
 GetAccessGrantsInstanceResourcePolicyResponse getResponse =
 s3Control.getAccessGrantsInstanceResourcePolicy(getRequest);
 LOGGER.info("GetAccessGrantsInstanceResourcePolicyResponse: " + getResponse);
 }
```

Réponse :

```
GetAccessGrantsInstanceResourcePolicyResponse(
 Policy={"Version":"2012-10-17","Statement":[{"Effect":"Allow","Principal":
{"AWS":"arn:aws:iam::444455556666:root"},"Action":
["s3:ListAccessGrants","s3:ListAccessGrantsLocations","s3:GetDataAccess","s3:GetAccessGrants
east-2:111122223333:access-grants/default"}]},
 CreatedAt=2023-06-15T22:54:44.319Z
 )
```

Example Supprimer une politique de ressources d'autorisations d'accès S3

Pour supprimer une politique de ressources d'autorisations d'accès S3, utilisez l'exemple de code suivant. Pour utiliser l'exemple de commande suivant, remplacez les *user input placeholders* par vos propres informations.

```
public void deleteAccessGrantsInstanceResourcePolicy() {
 DeleteAccessGrantsInstanceResourcePolicyRequest deleteRequest =
 DeleteAccessGrantsInstanceResourcePolicyRequest.builder()
 .accountId(111122223333)
```

```
.build();
DeleteAccessGrantsInstanceResourcePolicyResponse deleteResponse =
s3Control.putAccessGrantsInstanceResourcePolicy(deleteRequest);
LOGGER.info("DeleteAccessGrantsInstanceResourcePolicyResponse: " + deleteResponse);
}
```

Réponse :

```
DeleteAccessGrantsInstanceResourcePolicyResponse()
```

Étape 3 : accorder aux identités IAM d'un deuxième compte l'autorisation d'appeler l'instance d'autorisations d'accès S3 de votre compte

Une fois que le propriétaire des données Amazon S3 a configuré la politique intercompte pour l'instance d'autorisations d'accès S3 dans le compte `111122223333`, le propriétaire du deuxième compte `444455556666` doit créer une politique basée sur l'identité pour ses utilisateurs ou rôles IAM, et le propriétaire doit leur donner accès à l'instance d'autorisations d'accès S3. Dans la politique basée sur l'identité, incluez une ou plusieurs des actions suivantes, en fonction de ce qui est accordé dans la politique de ressources d'instance d'autorisations d'accès S3 et des autorisations que vous souhaitez accorder :

- `s3:ListAccessGrants`
- `s3:ListAccessGrantsLocations`
- `s3:GetDataAccess`
- `s3:GetAccessGrantsInstanceForPrefix`
- `s3:ListCallerAccessGrants`

Selon le modèle d'accès intercompte AWS, les utilisateurs ou rôles IAM du deuxième compte `444455556666` doivent explicitement disposer d'une ou de plusieurs de ces autorisations. Par exemple, accordez l'autorisation `s3:GetDataAccess` afin que l'utilisateur ou le rôle IAM puisse appeler l'instance d'autorisations d'accès S3 associée au compte `111122223333` pour demander des informations d'identification.

Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
{
```

```
 "Version": "2012-10-17",
 "Statement": [
 {
  "Effect": "Allow",
  "Action": [
   "s3:GetDataAccess",
  ],
   "Resource": "arn:aws:s3:us-east-2:111122223333:access-grants/default"
  }
 ]
}
```

Pour plus d'informations sur la modification d'une politique basée sur l'identité IAM, consultez Modification des politiques IAM dans le Guide AWS Identity and Access Management .

Étape 4 : créer une autorisation dans l'instance d'autorisations d'accès S3 de votre compte qui donne à l'identité IAM du deuxième compte l'accès à certaines de vos données S3

Pour l'étape finale de configuration, vous pouvez créer une autorisation dans l'instance d'autorisations d'accès S3 de votre compte 111122223333, qui donne accès à l'identité IAM du deuxième compte 444455556666 à certaines données S3 de votre compte. Vous pouvez le faire à l'aide de la console Amazon S3, de la CLI, de l'API et SDKs. Pour de plus amples informations, veuillez consulter Création d'octrois.

Dans l'autorisation, spécifiez l' AWS ARN de l'identité IAM du deuxième compte et spécifiez à quel emplacement dans vos données S3 (un compartiment, un préfixe ou un objet) vous accordez l'accès. Cet emplacement doit déjà être enregistré auprès de votre instance d'autorisations d'accès S3. Pour de plus amples informations, veuillez consulter Enregistrement d'un emplacement. Vous pouvez la possibilité de spécifier un sous-préfixe. Par exemple, si l'emplacement auquel vous accordez l'accès est un compartiment et que vous souhaitez limiter davantage l'accès à un objet spécifique de ce compartiment, transmettez le nom de la clé de l'objet dans le champ `S3SubPrefix`. Ou si vous souhaitez limiter l'accès aux objets du compartiment dont les noms de clé commencent par un préfixe spécifique tel que `2024-03-research-results/`, transmettez `S3SubPrefix=2024-03-research-results/`.

Voici un exemple de commande CLI permettant de créer une autorisation d'accès pour une identité dans le deuxième compte. Pour plus d'informations, consultez Création d'octrois. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control create-access-grant \
--account-id 111122223333 \
--access-grants-location-id default \
--access-grants-location-configuration S3SubPrefix=prefixA* \
--permission READ \
--grantee GranteeType=IAM,GranteeIdentifier=arn:aws:iam::444455556666:role/data-consumer-1
```

Après avoir configuré l'accès intercompte, l'utilisateur ou le rôle du deuxième compte peut effectuer les opérations suivantes :

- Appelle `ListAccessGrantsInstances` pour répertorier les instances d'autorisations d'accès S3 partagées avec ce service via AWS RAM. Pour de plus amples informations, veuillez consulter Obtention des détails d'une instance d'autorisations d'accès S3.
- Demande des informations d'identification temporaires auprès des autorisations d'accès S3. Pour découvrir comment effectuer ces demandes, consultez Demande d'un accès aux données Amazon S3 via les autorisations d'accès S3.

Gestion des balises pour les subventions d'accès S3

Dans les autorisations d'accès Amazon S3, les balises présentent des caractéristiques similaires à celles des balises d'objet dans Amazon S3. Chaque balise est une paire clés-valeurs. Les ressources que vous pouvez baliser dans les autorisations d'accès S3 sont les instances, les emplacements et les octrois.

> **Note**
>
> Le balisage dans les autorisations d'accès S3 utilise des opérations d'API différentes de celles du balisage d'objets. Les autorisations d'accès S3 utilisent les opérations d'API TagResource, UntagResource et ListTagsForResource, où une ressource peut être une instance d'autorisations d'accès S3, un emplacement enregistré ou une autorisation d'accès.

Comme avec les balises d'objet, les limitations suivantes s'appliquent :

- Vous pouvez ajouter des balises à de nouvelles ressources d'autorisations d'accès S3 lorsque vous les créez, ou vous pouvez ajouter des balises à des ressources existantes.

- Vous pouvez associer jusqu'à 10 balises à une ressource. Si plusieurs balises sont associées à la même ressource, elles doivent avoir des clés de balise uniques.
- Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les balises sont représentées en interne au format UTF-16. Dans le format UTF-16, les caractères occupent une ou deux positions de caractère.
- Les clés et les valeurs sont sensibles à la casse.

Pour plus d'informations sur les restrictions liées aux balises, consultez Restrictions encadrant les balises définies par l'utilisateur dans le Guide de l'utilisateur AWS Billing .

Vous pouvez baliser les ressources dans S3 Access Grants en utilisant le AWS Command Line Interface (AWS CLI), l'API REST Amazon S3 ou le AWS SDKs.

En utilisant le AWS CLI

Pour l'installer AWS CLI, reportez-vous à la section Installation du AWS CLI dans le guide de AWS Command Line Interface l'utilisateur.

Vous pouvez baliser une ressource d'autorisations d'accès S3 lorsque vous la créez ou après l'avoir créée. Les exemples suivants montrent comment baliser une instance d'autorisations d'accès S3 ou en annuler le balisage. Vous pouvez effectuer des opérations similaires pour des emplacements enregistrés et des autorisations d'accès.

Pour utiliser les exemples de commandes suivants, remplacez les *user input placeholders* par vos propres informations.

Example : Créer une instance d'autorisations d'accès S3 avec des balises

```
aws s3control create-access-grants-instance \
 --account-id 111122223333 \
 --profile access-grants-profile \
 --region us-east-2 \
 --tags Key=tagKey1,Value=tagValue1
```

Réponse :

```
 {
    "CreatedAt": "2023-10-25T01:09:46.719000+00:00",
    "AccessGrantsInstanceId": "default",
```

```
    "AccessGrantsInstanceArn": "arn:aws:s3:us-east-2:111122223333:access-grants/
default"
}
```

Example : Baliser une instance d'autorisations d'accès S3 déjà créée

```
aws s3control tag-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2 \
--tags Key=tagKey2,Value=tagValue2
```

Example : Répertorier les balises pour l'instance d'autorisations d'accès S3

```
aws s3control list-tags-for-resource \
--account-id 111122223333 \
--resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
--profile access-grants-profile \
--region us-east-2
```

Réponse :

```
{
    "Tags": [
        {
            "Key": "tagKey1",
            "Value": "tagValue1"
        },
        {
            "Key": "tagKey2",
            "Value": "tagValue2"
        }
    ]
}
```

Example : Annuler le balisage de l'instance d'autorisations d'accès S3

```
aws s3control untag-resource \
 --account-id 111122223333 \
 --resource-arn "arn:aws:s3:us-east-2:111122223333:access-grants/default" \
 --profile access-grants-profile \
```

```
--region us-east-2 \
--tag-keys "tagKey2"
```

Utilisation de l'API REST

Vous pouvez utiliser l'API Amazon S3 pour définir des balises, annuler le balisage ou répertorier les balises pour une instance d'autorisations d'accès S3, un emplacement enregistré ou une autorisation d'accès. Pour en savoir plus sur la prise en charge de l'API REST pour la gestion des balises d'autorisations d'accès S3, consultez les sections suivantes dans la Référence d'API Amazon Simple Storage Service :

- TagResource
- UntagResource
- ListTagsForResource

Limitations des autorisations d'accès S3

Les autorisations d'accès S3 présentent les limitations suivantes :

> **Note**
>
> Si votre cas d'utilisation dépasse ces limites, contactez le AWS support pour demander des limites plus élevées.

Instance d'autorisations d'accès S3

Vous pouvez créer une instance S3 Access Grants Région AWS par compte. Consultez Création d'une instance d'autorisations d'accès S3.

Emplacement d'autorisations d'accès S3

Vous pouvez enregistrer 1 000 emplacements d'autorisations d'accès S3 par instance d'autorisations d'accès S3. Consultez Enregistrement d'un emplacement d'autorisations d'accès S3.

Octroi

Vous pouvez créer 100 000 octrois par instance d'autorisations d'accès S3. Consultez Création d'un octroi.

Subventions d'accès S3 Régions AWS

S3 Access Grants est actuellement disponible dans les versions suivantes Régions AWS :

Région AWS code	Région AWS nom
us-east-1	USA Est (Virginie du Nord)
us-east-2	USA Est (Ohio)
us-west-1	USA Ouest (Californie du Nord)
us-west-2	USA Ouest (Oregon)
af-south-1	Afrique (Le Cap)
ap-east-1	Asie-Pacifique (Hong Kong)
ap-northeast-1	Asie-Pacifique (Tokyo)
ap-northeast-2	Asie-Pacifique (Séoul)
ap-northeast-3	Asie-Pacifique (Osaka)
ap-south-1	Asie-Pacifique (Mumbai)
ap-south-2	Asie-Pacifique (Hyderabad)
ap-southeast-1	Asie-Pacifique (Singapour)
ap-southeast-2	Asie-Pacifique (Sydney)
ap-southeast-3	Asie-Pacifique (Jakarta)
ap-southeast-4	Asie-Pacifique (Melbourne)
ca-central-1	Canada (Centre)
ca-west-1	Canada-Ouest (Calgary)
eu-central-1	Europe (Francfort)

Région AWS code	Région AWS nom
eu-central-2	Europe (Zurich)
eu-north-1	Europe (Stockholm)
eu-south-1	Europe (Milan)
eu-south-2	Europe (Espagne)
eu-west-1	Europe (Irlande)
eu-west-2	Europe (Londres)
eu-west-3	Europe (Paris)
il-central-1	Israël (Tel Aviv)
me-central-1	Moyen-Orient (EAU)
me-south-1	Moyen-Orient (Bahreïn)
sa-east-1	Amérique du Sud (São Paulo)
us-gov-east-1	AWS GovCloud (USA Est)
us-gov-west-1	AWS GovCloud (US-Ouest)

Intégrations des autorisations d'accès S3

Les subventions d'accès S3 peuvent être utilisées avec les AWS services et fonctionnalités suivants. Cette page sera mise à jour au fur et à mesure que de nouvelles intégrations seront disponibles.

> **Tip**
>
> Cet AWS atelier consacré aux subventions d'accès S3 vous explique comment utiliser les subventions d'accès S3 avec les utilisateurs AWS Identity and Access Management (IAM), les utilisateurs d'IAM Identity Center, Amazon EMR et. AWS Transfer Family

Amazon Athena

Utilisation des groupes de travail Athena compatibles avec IAM Identity Center

Amazon EMR

Lancement d'un cluster Amazon EMR avec les autorisations d'accès S3

Amazon EMR on EKS

Lancement d'un cluster Amazon EMR sur EKS avec les autorisations d'accès S3

Application Amazon EMR sans serveur

Lancement d'une application Amazon EMR sans serveur avec les autorisations d'accès S3

Amazon Redshift

Intégration d'Amazon Redshift aux autorisations d'accès Amazon S3

Amazon SageMaker AI Studio

Ajout de données Amazon S3 à Amazon SageMaker AI Unified Studio

Grâce aux subventions d'accès S3 dans Amazon SageMaker AI Unified Studio, vous pouvez partager vos données Amazon S3 dans le cadre de plusieurs projets. Pour autoriser l'accès aux données à l'aide de S3 Access Grants, une instance S3 Access Grants est requise. Amazon SageMaker AI Unified Studio utilisera une instance S3 Access Grants si une instance est déjà disponible ou s'il est possible de créer une instance. Tout d'abord, vous ajoutez vos données Amazon S3, puis vous les publiez dans le catalogue ou vous les partagez directement avec les consommateurs.

Utilisation d'Amazon S3 Access Grants avec Amazon SageMaker AI Studio et le plugin SDK pour Python (Boto3)

Il est désormais plus facile d'utiliser S3 Access Grants dans les blocs-notes Amazon SageMaker AI Studio avec le plugin SDK for Python (Boto3). Configurez au préalable les autorisations d'accès pour les principaux IAM et les utilisateurs de l' AWS IAM Identity Center annuaire. Bien qu'Amazon SageMaker AI Studio ne prenne pas en charge de manière native les utilisateurs de l'annuaire des fournisseurs d'identité, vous pouvez écrire du code Python personnalisé à l'aide du plugin qui permet à ces identités d'accéder aux données S3 via S3 Access Grants. L'accès aux données s'effectue à l'aide du plugin et non via Amazon SageMaker AI.

AWS Glue

Subventions d'accès Amazon S3 avec AWS Glue

AWS IAM Identity Center

- Propagation d'identité approuvée entre applications

AWS Transfer Family

- Configurer les autorisations d'accès Amazon S3 pour AWS Transfer Family

Navigateur de stockage pour S3

- Gestion de l'accès aux données à l'échelle à l'aide du navigateur de stockage pour S3

Frameworks Python open source

- Les autorisations d'accès Amazon S3 s'intègrent désormais aux frameworks Python open source

Gérer l'accès avec ACLs

Les listes de contrôle d'accès (ACLs) sont l'une des options basées sur les ressources que vous pouvez utiliser pour gérer l'accès à vos compartiments et objets. Vous pouvez l'utiliser ACLs pour accorder des autorisations de lecture/écriture de base à d'autres personnes. Comptes AWS Il existe des limites à la gestion des autorisations à l'aide de ACLs.

Par exemple, vous ne pouvez accorder des autorisations qu'à d'autres personnes Comptes AWS ; vous ne pouvez pas accorder d'autorisations aux utilisateurs de votre compte. Vous ne pouvez pas accorder d'autorisations conditionnelles, ni refuser explicitement des autorisations. ACLs sont adaptés à des scénarios spécifiques. Par exemple, si le propriétaire d'un compartiment autorise d'autres personnes Comptes AWS à télécharger des objets, les autorisations relatives à ces objets ne peuvent être gérées Compte AWS que par le propriétaire de l'objet à l'aide de l'ACL de l'objet.

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès à ceux-ci exclusivement à l'aide de politiques de gestion des accès.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre

compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

> **Important**
>
> Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Pour plus d'informations ACLs, consultez les rubriques suivantes.

Rubriques

- Présentation de la liste de contrôle d'accès (ACL)
- Configuration ACLs
- Exemples de politiques pour ACLs

Présentation de la liste de contrôle d'accès (ACL)

Les listes de contrôle d'accès Amazon S3 (ACLs) vous permettent de gérer l'accès aux compartiments et aux objets. Chaque compartiment et objet possède une liste ACL qui lui est attachée comme sous-ressource. Il définit le Comptes AWS ou les groupes auxquels l'accès est accordé et le type d'accès. Lors de la réception d'une demande sur une ressource, Amazon S3 vérifie la liste ACL correspondante pour s'assurer que le demandeur possède les autorisations d'accès nécessaires.

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès à ceux-ci exclusivement à l'aide de politiques de gestion des accès.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

> **Important**
>
> Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Lorsque vous créez un compartiment ou un objet, Amazon S3 crée une liste ACL par défaut qui octroie au propriétaire de la ressource le contrôle total sur celle-ci. Ce comportement est illustré dans l'exemple de liste ACL de compartiment suivant (la liste ACL d'objet par défaut possède la même structure) :

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Owner>
    <ID>*** Owner-Canonical-User-ID ***</ID>
    <DisplayName>owner-display-name</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:type="Canonical User">
        <ID>*** Owner-Canonical-User-ID ***</ID>
        <DisplayName>display-name</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
```

```
    </Grant>
  </AccessControlList>
</AccessControlPolicy>
```

L'exemple de liste ACL inclut un élément `Owner` qui identifie le propriétaire par l'ID d'utilisateur canonique du Compte AWS. Pour obtenir des instructions pour trouver votre ID d'utilisateur canonique, consultez Trouver un nom d'utilisateur Compte AWS canonique. L'`Grant`élément identifie le bénéficiaire (soit un groupe prédéfini, Compte AWS soit un groupe prédéfini) et l'autorisation accordée. Cette liste ACL par défaut possède un élément `Grant` pour le propriétaire. Vous accordez des autorisations en ajoutant des éléments `Grant`, avec chaque accord identifiant le bénéficiaire et l'autorisation.

> **Note**
>
> Une liste ACL peut avoir 100 accords maximum.

Rubriques

- Qui est un bénéficiaire ?
- Quelles autorisations puis-je octroyer ?
- Valeurs aclRequired pour les demandes Amazon S3 courantes
- Exemple de liste ACL
- Liste ACL prête à l'emploi

Qui est un bénéficiaire ?

> **Important**
>
> Avis de fin de support : à compter du 1er octobre 2025, Amazon S3 cessera de prendre en charge la création de nouvelles listes de contrôle d'accès (ACL) des bénéficiaires du courrier électronique. Le bénéficiaire du courrier électronique ACLs créé avant cette date continuera de fonctionner et restera accessible via la console de AWS gestion, l'interface de ligne de commande (CLI) et l'API REST. SDKs Cependant, vous ne serez plus en mesure de créer un nouveau bénéficiaire ACLs par e-mail.
>
> Entre le 15 juillet 2025 et le 1er octobre 2025, vous commencerez à constater une augmentation du nombre d'`HTTP 405`erreurs liées aux demandes adressées à Amazon S3 lorsque vous tenterez de créer un nouveau bénéficiaire ACLs par e-mail.

Ce changement concerne les régions suivantes Régions AWS : USA Est (Virginie du Nord), USA Ouest (Californie du Nord), USA Ouest (Oregon), Asie-Pacifique (Singapour), Asie-Pacifique (Sydney), Asie-Pacifique (Tokyo), Europe (Irlande) et Amérique du Sud (São Paulo).

Un bénéficiaire peut être un Compte AWS ou l'un des groupes Amazon S3 prédéfinis. Vous autorisez l' Compte AWS utilisation de l'adresse e-mail ou de l'ID utilisateur canonique. Toutefois, si vous fournissez une adresse e-mail dans la demande d'accord, Amazon S3 trouve l'ID d'utilisateur canonique pour ce compte et l'ajoute à la liste ACL. Le résultat contient ACLs toujours l'ID utilisateur canonique du Compte AWS, et non l'adresse e-mail du Compte AWS.

Lorsque vous accordez des droits d'accès, vous spécifiez chaque bénéficiaire sous la forme d'une paire *`type`*`="`*`value`*`"`, où le *`type`* est l'un des suivants :

- `id`— Si la valeur spécifiée est l'ID utilisateur canonique d'un Compte AWS
- `uri` : si vous accordez des autorisations à un groupe prédéfini
- `emailAddress` : si la valeur spécifiée est l'adresse e-mail d'un Compte AWS

Important

L'utilisation d'adresses e-mail pour spécifier un bénéficiaire est prise en charge uniquement dans les Régions AWS suivantes :

- US East (N. Virginia)
- USA Ouest (Californie du Nord)
- US West (Oregon)
- Asie-Pacifique (Singapour)
- Asie-Pacifique (Sydney)
- Asia Pacific (Tokyo)
- Europe (Ireland)
- South America (São Paulo)

Pour obtenir la liste de toutes les régions et de tous les points de terminaison Amazon S3 pris en charge, consultez Régions et points de terminaison dans Référence générale d'Amazon Web Services.

Example Exemple : adresse e-mail

Par exemple, l'`x-amz-grant-read`en-tête suivant accorde aux adresses e-mail Comptes AWS identifiées l'autorisation de lire les données des objets et leurs métadonnées :

```
x-amz-grant-read: emailAddress="xyz@example.com", emailAddress="abc@example.com"
```

Warning

Lorsque vous accordez à d'autres personnes l' Comptes AWS accès à vos ressources, sachez qu'elles Comptes AWS peuvent déléguer leurs autorisations aux utilisateurs de leurs comptes. Il s'agit d'un accès intercompte. Pour en savoir plus sur l'utilisation de l'accès intercompte, consultez Création d'un rôle pour la délégation d'autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM.

Trouver un nom d'utilisateur Compte AWS canonique

L'ID d'utilisateur canonique est associé au Compte AWS. Cet ID est composé d'une longue chaîne de caractères, par exemple :

`79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be`

Pour découvrir comment trouver l'ID d'utilisateur canonique de votre compte, consultez Recherche de l'ID d'utilisateur canonique de votre Compte AWS dans le Guide de référence sur la gestion des comptes AWS .

Vous pouvez également rechercher l'ID utilisateur canonique d'un Compte AWS en lisant l'ACL d'un bucket ou d'un objet auquel il Compte AWS possède des autorisations d'accès. Lorsqu'une personne Compte AWS obtient des autorisations par le biais d'une demande de subvention, une entrée de subvention est ajoutée à l'ACL avec l'ID utilisateur canonique du compte.

> **Note**
>
> Si vous rendez votre compartiment public (non recommandé), n'importe quel utilisateur non authentifié pourra y charger des objets. Ces utilisateurs anonymes ne disposent pas d'un Compte AWS. Lorsqu'un utilisateur anonyme charge un objet dans votre compartiment, Amazon S3 ajoute un ID utilisateur canonique spécial (`65a011a29cdf8ec533ec3d1ccaae921c`) comme propriétaire de l'objet dans la liste ACL. Pour plus d'informations, consultez Propriété du compartiment et de l'objet Amazon S3.

Groupes prédéfinis Amazon S3

Amazon S3 possède un ensemble de groupes prédéfinis. Lorsque vous accordez l'accès à un compte à un groupe, vous spécifiez l'un des Amazon S3 URIs au lieu d'un ID utilisateur canonique. Amazon S3 fournit les groupes prédéfinis suivants :

- Groupe des utilisateurs authentifiés – Représenté par `http://acs.amazonaws.com/groups/global/AuthenticatedUsers`.

  Ce groupe représente tout le monde Comptes AWS. L'autorisation d'accès à ce groupe permet Compte AWS à n'importe qui d'accéder à la ressource. Toutefois, toutes les demandes doivent être signées (authentifiées).

  > **Warning**
  >
  > Lorsque vous accordez l'accès au groupe Utilisateurs authentifiés, n'importe quel utilisateur AWS authentifié dans le monde peut accéder à votre ressource.

- Groupe de tous les utilisateurs – Représenté par `http://acs.amazonaws.com/groups/global/AllUsers`.

  Une autorisation d'accès à ce groupe permet à tout le monde d'accéder à la ressource. Les demandes peuvent être signées (authentifiées) ou non (anonymes). Les demandes non signées omettent l'en-tête Authentification dans la demande.

  > **Warning**
  >
  > Nous vous recommandons vivement de ne pas jamais accorder au groupe de tous les utilisateurs les autorisations `WRITE`, `WRITE_ACP` ou `FULL_CONTROL`. Par exemple,

bien que `WRITE` les autorisations empêchent les non-propriétaires de remplacer ou de supprimer des objets existants, `WRITE` les autorisations permettent toujours à quiconque de stocker des objets dans votre compartiment, pour lesquels vous êtes facturé. Pour plus de détails sur ces autorisations, consultez la section Quelles autorisations puis-je octroyer ? suivante.

- Groupe de livraison des journaux – Représenté par `http://acs.amazonaws.com/groups/s3/LogDelivery`.

  Une autorisation `WRITE` sur un compartiment permet à ce groupe d'écrire des journaux d'accès au serveur (consultez Enregistrement de demandes avec journalisation des accès au serveur) dans le compartiment.

> **Note**
>
> Lors de l'utilisation ACLs, un bénéficiaire peut être un Compte AWS ou l'un des groupes Amazon S3 prédéfinis. Toutefois, le bénéficiaire ne peut pas être un utilisateur IAM. Pour plus d'informations sur les utilisateurs et autorisations AWS dans IAM, consultez Utilisation d' AWS Identity and Access Management.

Quelles autorisations puis-je octroyer ?

Le tableau suivant répertorie l'ensemble des autorisations qu'Amazon S3 prend en charge dans une liste ACL. Toutes les autorisations de liste ACL sont identiques pour les listes ACL d'objet et de compartiment. Toutefois, selon le contexte (liste ACL de compartiment ou liste ACL d'objet), ces autorisations de liste ACL accordent des autorisations pour des opérations spécifiques de compartiment ou d'objet. Le tableau répertorie les autorisations et décrit ce qu'elles signifient pour des objets et des compartiments.

Pour plus d'informations sur les autorisations ACL dans la console Amazon S3, consultez Configuration ACLs.

Autorisations	Lorsqu'elles sont accordées sur un compartiment	Lorsqu'elles sont accordées sur un objet
`READ`	Elles permettent au bénéficiaire de répertorier les objets dans le compartiment	Elles permettent au bénéficiaire de lire les données de l'objet et ses métadonnées
`WRITE`	Elles permettent au bénéficiaire de créer des objets dans le compartiment. Pour les propriétaires de compartiments et d'objets existants, elles permettent également de supprimer et de remplacer ces objets.	Ne s'applique pas
`READ_ACP`	Elles permettent au bénéficiaire de lire la liste ACL du compartiment	Elles permettent au bénéficiaire de lire la liste ACL de l'objet
`WRITE_ACP`	Elles permettent au bénéficiaire d'écrire la liste ACL pour le compartiment applicable	Elles permettent au bénéficiaire d'écrire la liste ACL pour l'objet applicable
`FULL_CONTROL`	Elle accorde au bénéficiaire les autorisations `READ`, `WRITE`, `READ_ACP` et `WRITE_ACP` sur le compartiment	Elle accorde au bénéficiaire les autorisations `READ`, `READ_ACP` et `WRITE_ACP` sur l'objet

Warning

Soyez vigilant lorsque vous accordez des autorisations d'accès à vos compartiments et objets S3. Par exemple, l'octroi de l'accès `WRITE` à un compartiment permet au bénéficiaire de créer des objets dans le compartiment. Nous vous recommandons vivement de lire l'ensemble de la section Présentation de la liste de contrôle d'accès (ACL) avant d'accorder des autorisations.

Mappage des autorisations de liste ACL et de stratégie d'accès

Comme illustré dans la table précédente, une liste ACL permet uniquement d'accorder un ensemble limité d'autorisations, comparé au nombre d'autorisations configurables dans une stratégie d'accès (consultez Actions de politique pour Amazon S3). Chacune de ces autorisations permet une ou plusieurs opérations Amazon S3.

Le tableau suivant montre comment chacune des autorisations de liste ACL est mappée aux autorisations de stratégie d'accès correspondantes. Comme vous pouvez le voir, une stratégie d'accès accorde plus d'autorisations qu'une liste ACL. Vous l'utilisez ACLs principalement pour accorder read/write des autorisations de base, similaires aux autorisations de système de fichiers. Pour plus d'informations sur le moment où utiliser une ACL, consultez Gestion des identités et des accès pour Amazon S3.

Pour plus d'informations sur les autorisations ACL dans la console Amazon S3, consultez Configuration ACLs.

Autorisation de liste ACL	Autorisations de stratégie d'accès correspondantes lorsqu'une autorisation de liste ACL est accordée sur un compartiment	Autorisations de stratégie d'accès correspondantes lorsqu'une autorisation de liste ACL est accordée sur un objet
`READ`	`s3:ListBucket` , `s3:ListBucketVersions` et `s3:ListBucketMultipartUploads`	`s3:GetObject` et `s3:GetObjectVersion`
`WRITE`	`s3:PutObject` Le propriétaire du compartiment peut créer, remplacer et supprimer n'importe quel objet dans le compartiment, et le propriétaire de l'objet bénéficie du `FULL_CONTROL` sur son objet. De plus, lorsque le bénéficiaire est le propriétaire du compartiment, l'accord d'une autorisation `WRITE` dans la liste ACL d'un compartiment permet	Ne s'applique pas

Autorisation de liste ACL	Autorisations de stratégie d'accès correspondantes lorsqu'une autorisation de liste ACL est accordée sur un compartiment	Autorisations de stratégie d'accès correspondantes lorsqu'une autorisation de liste ACL est accordée sur un objet
	d'exécuter l'action `s3:DeleteObjectVersion` sur n'importe quelle version de ce compartiment.	
`READ_ACP`	`s3:GetBucketAcl`	`s3:GetObjectAcl` et `s3:GetObjectVersionAcl`
`WRITE_ACP`	`s3:PutBucketAcl`	`s3:PutObjectAcl` et `s3:PutObjectVersionAcl`
`FULL_CONTROL`	Équivaut à accorder les autorisations de liste ACL `READ`, `WRITE`, `READ_ACP` et `WRITE_ACP`. Par conséquent, cette autorisation de liste ACL est mappée à une combinaison d'autorisations de stratégie d'accès correspondantes.	Équivaut à accorder les autorisations de liste ACL `READ`, `READ_ACP` et `WRITE_ACP`. Par conséquent, cette autorisation de liste ACL est mappée à une combinaison d'autorisations de stratégie d'accès correspondantes.

Clés de condition

Lorsque vous accordez des autorisations de stratégie d'accès, vous pouvez utiliser des clés de condition pour limiter la valeur de l'ACL sur un objet à l'aide d'une politique de compartiment. Les clés de contexte suivantes correspondent à ACLs. Vous pouvez utiliser ces clés de contexte pour exiger l'utilisation d'une liste ACL spécifique dans une demande :

- `s3:x-amz-grant-read` - Exiger un accès en lecture.
- `s3:x-amz-grant-write` - Exiger un accès en écriture.
- `s3:x-amz-grant-read-acp` - Exiger un accès en lecture à l'ACL du compartiment.
- `s3:x-amz-grant-write-acp` - Exiger un accès en écriture à l'ACL du compartiment.
- `s3:x-amz-grant-full-control` - Exiger un contrôle total.
- `s3:x-amz-acl` - Exiger une Liste ACL prête à l'emploi.

Pour des exemples de stratégies impliquant des en-têtes spécifiques à une liste ACL, consultez Octroi de s3 : PutObject autorisation assortie d'une condition obligeant le propriétaire du bucket à obtenir le contrôle total. Pour obtenir la liste complète des clés de condition spécifiques à Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Valeurs **`aclRequired`** pour les demandes Amazon S3 courantes

Pour identifier les demandes Amazon S3 nécessitant ACLs une autorisation, vous pouvez utiliser la `aclRequired` valeur dans les journaux d'accès au serveur Amazon S3 ou AWS CloudTrail. La `aclRequired` valeur qui apparaît dans les journaux CloudTrail d'accès au serveur Amazon S3 dépend des opérations appelées et de certaines informations concernant le demandeur, le propriétaire de l'objet et le propriétaire du compartiment. Si aucune valeur ACLs n'est requise, ou si vous définissez l'ACL `bucket-owner-full-control` prédéfinie, ou si les demandes sont autorisées par votre politique de compartiment, la chaîne de `aclRequired` valeur est « `-` » dans les journaux d'accès au serveur Amazon S3 et est absente dans CloudTrail.

Les tableaux suivants répertorient les `aclRequired` valeurs attendues dans les journaux CloudTrail d'accès au serveur Amazon S3 pour les différentes opérations d'API Amazon S3. Vous pouvez utiliser ces informations pour comprendre de quelles opérations Amazon S3 dépendent ACLs pour obtenir une autorisation. Dans les tables suivantes, A, B et C représentent les différents comptes associés au demandeur, au propriétaire de l'objet et au propriétaire du compartiment. Les entrées suivies d'un astérisque (*) indiquent l'un des comptes A, B ou C.

> **Note**
>
> Les opérations `PutObject` de la table suivante, sauf indication contraire, indiquent les demandes qui ne définissent pas de liste ACL, sauf si la liste ACL est `bucket-owner-full-control`. Une valeur nulle pour `aclRequired` indique qu'il `aclRequired` est absent des AWS CloudTrail journaux.

Le tableau suivant indique les `aclRequired` valeurs de CloudTrail.

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`GetObject`	A	A	A	Oui ou Non	null	Accès dans le même compte
`GetObject`	A	B	A	Oui ou Non	null	Accès au même compte avec le propriétaire du compartiment obligatoire
`GetObject`	A	A	B	Oui	null	Accès intercompte accordé par la politique du compartiment
`GetObject`	A	A	B	Non	Oui	Accès intercompte reposant sur la liste ACL

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`GetObject`	A	A	B	Oui	null	Accès intercompte accordé par la politique du compartiment
`GetObject`	A	B	B	Non	Oui	Accès intercompte reposant sur la liste ACL
`GetObject`	A	B	C	Oui	null	Accès intercompte accordé par la politique du compartiment
`GetObject`	A	B	C	Non	Oui	Accès intercompte reposant sur la liste ACL

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`PutObject`	A	Ne s'applique pas	A	Oui ou Non	null	Accès dans le même compte
`PutObject`	A	Ne s'applique pas	B	Oui	null	Accès intercompte accordé par la politique du compartiment
`PutObject`	A	Ne s'applique pas	B	Non	Oui	Accès intercompte reposant sur la liste ACL
`PutObject` avec une liste ACL (sauf pour `bucket-owner-full-control`)	*	Ne s'applique pas	*	Oui ou Non	Oui	Demande autorise la liste ACL

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`ListObjects`	A	Ne s'applique pas	A	Oui ou Non	null	Accès dans le même compte
`ListObjects`	A	Ne s'applique pas	B	Oui	null	Accès intercompte accordé par la politique du compartiment
`ListObjects`	A	Ne s'applique pas	B	Non	Oui	Accès intercompte reposant sur la liste ACL
`DeleteObject`	A	Ne s'applique pas	A	Oui ou Non	null	Accès dans le même compte

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`DeleteObject`	A	Ne s'applique pas	B	Oui	null	Accès intercompte accordé par la politique du compartiment
`DeleteObject`	A	Ne s'applique pas	B	Non	Oui	Accès intercompte reposant sur la liste ACL
`PutObjectAcl`	*	*	*	Oui ou Non	Oui	Demande autorise la liste ACL
`PutBucketAcl`	*	Ne s'applique pas	*	Oui ou Non	Oui	Demande autorise la liste ACL

> **Note**
>
> Les opérations `REST.PUT.OBJECT` de la table suivante, sauf indication contraire, indiquent les demandes qui ne définissent pas de liste ACL, sauf si la liste ACL est `bucket-owner-full-control`. Une chaîne de valeur `aclRequired` « `-` » indique une valeur nulle dans les journaux d'accès au serveur Amazon S3.

Le tableau suivant indique les valeurs `aclRequired` des journaux d'accès au serveur Amazon S3.

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`REST.GET.OBJECT`	A	A	A	Oui ou Non	-	Accès dans le même compte
`REST.GET.OBJECT`	A	B	A	Oui ou Non	-	Accès au même compte avec le propriétaire du compartiment obligatoire
`REST.GET.OBJECT`	A	A	B	Oui	-	Accès intercompte accordé par la politique du compartiment
`REST.GET.OBJECT`	A	A	B	Non	Oui	Accès intercompte reposant sur la liste ACL

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`REST.GET.OBJECT`	A	B	B	Oui	-	Accès intercompte accordé par la politique du compartiment
`REST.GET.OBJECT`	A	B	B	Non	Oui	Accès intercompte reposant sur la liste ACL
`REST.GET.OBJECT`	A	B	C	Oui	-	Accès intercompte accordé par la politique du compartiment
`REST.GET.OBJECT`	A	B	C	Non	Oui	Accès intercompte reposant sur la liste ACL

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`REST.PUT.OBJECT`	A	Ne s'applique pas	A	Oui ou Non	-	Accès dans le même compte
`REST.PUT.OBJECT`	A	Ne s'applique pas	B	Oui	-	Accès intercompte accordé par la politique du compartiment
`REST.PUT.OBJECT`	A	Ne s'applique pas	B	Non	Oui	Accès intercompte reposant sur la liste ACL
`REST.PUT.OBJECT` avec une liste ACL (sauf pour `bucket-owner-full-control`)	*	Ne s'applique pas	*	Oui ou Non	Oui	Demande autorise la liste ACL

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **`aclRequired`**	Raison
`REST.GET.BUCKET`	A	Ne s'applique pas	A	Oui ou Non	-	Accès dans le même compte
`REST.GET.BUCKET`	A	Ne s'applique pas	B	Oui	-	Accès intercompte accordé par la politique du compartiment
`REST.GET.BUCKET`	A	Ne s'applique pas	B	Non	Oui	Accès intercompte reposant sur la liste ACL
`REST.DELETE.OBJECT`	A	Ne s'applique pas	A	Oui ou Non	-	Accès dans le même compte

Nom de l'opération	Demandeur	Propriétaire de l'objet	Propriétaire du compartiment	La politique du compartiment autorise l'accès	Valeur **aclRequired**	Raison
REST.DELETE.OBJECT	A	Ne s'applique pas	B	Oui	-	Accès intercompte accordé par la politique du compartiment
REST.DELETE.OBJECT	A	Ne s'applique pas	B	Non	Oui	Accès intercompte reposant sur la liste ACL
REST.PUT.ACL	*	*	*	Oui ou Non	Oui	Demande autorise la liste ACL

Exemple de liste ACL

L'exemple de liste ACL suivant sur un compartiment identifie le propriétaire de la ressource et un ensemble d'accords. Le format est la représentation XML d'une liste ACL dans l'API REST Amazon S3. Le propriétaire du compartiment possède l'accès FULL_CONTROL sur la ressource. En outre, l'ACL montre comment les autorisations sont accordées sur une ressource à deux Comptes AWS, identifiés par un ID utilisateur canonique, et à deux des groupes Amazon S3 prédéfinis décrits dans la section précédente.

Example

```
<?xml version="1.0" encoding="UTF-8"?>
<AccessControlPolicy xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
 <Owner>
   <ID>Owner-canonical-user-ID</ID>
   <DisplayName>display-name</DisplayName>
 </Owner>
 <AccessControlList>
   <Grant>
     <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
       <ID>Owner-canonical-user-ID</ID>
       <DisplayName>display-name</DisplayName>
     </Grantee>
     <Permission>FULL_CONTROL</Permission>
   </Grant>

   <Grant>
     <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
       <ID>user1-canonical-user-ID</ID>
       <DisplayName>display-name</DisplayName>
     </Grantee>
     <Permission>WRITE</Permission>
   </Grant>

   <Grant>
     <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="CanonicalUser">
       <ID>user2-canonical-user-ID</ID>
       <DisplayName>display-name</DisplayName>
     </Grantee>
     <Permission>READ</Permission>
   </Grant>

   <Grant>
     <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
       <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
     </Grantee>
     <Permission>READ</Permission>
   </Grant>
   <Grant>
     <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="Group">
       <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
     </Grantee>
     <Permission>WRITE</Permission>
   </Grant>
```

```
  </AccessControlList>
</AccessControlPolicy>
```

Liste ACL prête à l'emploi

Amazon S3 prend en charge un ensemble de subventions prédéfinies, appelées « standardisées ACLs ». Chaque liste ACL prête à l'emploi possède un ensemble prédéfini de bénéficiaires et d'autorisations. Le tableau suivant répertorie l'ensemble des autorisations prédéfinies ACLs et les autorisations prédéfinies associées.

Liste ACL prête à l'emploi	S'appliqu e à	Autorisations ajoutées à la liste ACL
`private`	Compartim ent et objet	Le propriétaire obtient l'accès `FULL_CONTROL` . Personne d'autre ne possède les droits d'accès (par défaut).
`public-read`	Compartim ent et objet	Le propriétaire obtient l'accès `FULL_CONTROL` . Le groupe `AllUsers` (consultez Qui est un bénéficiaire ?) obtient l'accès `READ`.
`public-read-write`	Compartim ent et objet	Le propriétaire obtient l'accès `FULL_CONTROL` . Le groupe `AllUsers` obtient l'accès `READ` et `WRITE`. L'accord de ce type d'accès sur un compartiment n'est généralement pas recommandé.
`aws-exec-read`	Compartim ent et objet	Le propriétaire obtient l'accès `FULL_CONTROL` . Amazon EC2 a `READ` accès à `GET` un bundle Amazon Machine Image (AMI) depuis Amazon S3.
`authenticated-read`	Compartim ent et objet	Le propriétaire obtient l'accès `FULL_CONTROL` . Le groupe `AuthenticatedUsers` obtient l'accès `READ`.
`bucket-owner-read`	Objet	Le propriétaire de l'objet obtient l'accès `FULL_CONTROL` . Le propriétaire du compartiment obtient l'accès `READ`. Si vous spécifiez cette ACL prédéfinie lors de la création du compartiment, Amazon S3 l'ignore.

Liste ACL prête à l'emploi	S'appliqu e à	Autorisations ajoutées à la liste ACL
`bucket-owner-full-control`	Objet	Le propriétaire de l'objet et celui du compartiment obtiennent l'accès `FULL_CONTROL` sur l'objet. Si vous spécifiez cette ACL prédéfinie lors de la création du compartiment, Amazon S3 l'ignore.
`log-delivery-write`	Compartim ent	Le groupe `LogDelivery` obtient les autorisations `WRITE` et `READ_ACP` sur le compartiment. Pour plus d'informations sur les journaux, consultez (Enregistr ement de demandes avec journalisation des accès au serveur).

> **Note**
>
> Vous ne pouvez spécifier qu'une seule de ces options ACLs prédéfinies dans votre demande.

Vous pouvez spécifier une liste ACL prédéfinie dans votre demande grâce à l'en-tête `x-amz-acl`. Lorsqu'Amazon S3 reçoit une demande contenant une liste ACL prédéfinie, il ajoute les accords prédéfinis à la liste ACL de la ressource.

Configuration ACLs

Cette section explique comment gérer les autorisations d'accès pour les compartiments et objets S3 à l'aide de listes de contrôle d'accès (ACLs). Vous pouvez ajouter des autorisations à votre ACL de ressources à l'aide de l'API AWS Management Console, AWS Command Line Interface (CLI), REST ou AWS SDKs.

Les autorisations de compartiment et d'objet sont indépendantes les unes des autres. un objet n'hérite pas des autorisations de son compartiment. Par exemple, si vous créez un compartiment et accordez un accès en écriture à un utilisateur, vous ne pouvez pas accéder à ses objets sauf s'il vous accorde explicitement l'accès.

Vous pouvez accorder des autorisations à d'autres Compte AWS utilisateurs ou à des groupes prédéfinis. L'utilisateur ou le groupe auquel vous accordez des autorisations est le « bénéficiaire ».

Par défaut, le propriétaire, qui a créé le compartiment, dispose des autorisations complètes. Compte AWS

Chaque autorisation accordée pour un utilisateur ou un groupe ajoute une entrée dans la liste ACL associée au compartiment. Les listes ACL répertorient le bénéficiaire et l'autorisation accordée.

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès à ceux-ci exclusivement à l'aide de politiques de gestion des accès.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Important

Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Warning

Nous vous recommandons vivement d'éviter d'accorder un accès en écriture aux groupes Tout le monde (accès public) ou Utilisateurs authentifiés (tous les utilisateurs AWS authentifiés). Pour en savoir plus sur les effets de l'octroi d'un accès en écriture à ces groupes, consultez Groupes prédéfinis Amazon S3.

Utilisation de la console S3 pour définir des autorisations ACL pour un compartiment

La console affiche les autorisations d'accès combinées pour les bénéficiaires en double. Pour voir la liste complète des ACLs, utilisez l'API REST Amazon S3 AWS CLI, ou AWS SDKs.

Le tableau suivant présente les autorisations ACL que vous pouvez configurer pour les compartiments dans la console Amazon S3.

Autorisations ACL de la console Amazon S3 pour les compartiments

Autorisation de la console	Autorisation de liste ACL	Accès
Objets – Liste	`READ`	Elles permettent au bénéficiaire de répertorier les objets dans le compartiment.
Objets – Écriture	`WRITE`	Elles permettent au bénéficiaire de créer des objets dans le compartiment. Pour les propriétaires de compartiments et d'objets existants, elles permettent également de supprimer et de remplacer ces objets.
ACL de compartiment – Lecture	`READ_ACP`	Elles permettent au bénéficiaire de lire la liste ACL du compartiment.
ACL de compartiment – Écriture	`WRITE_ACP`	Elles permettent au bénéficiaire d'écrire la liste ACL pour le compartiment applicable.
Tout le monde (accès public) : Objets – Liste	`READ`	Elles accordent un accès public en lecture pour les objets se trouvant dans le compartiment. Lorsque vous accordez l'accès à la liste à Tout le monde (accès public), quiconque dans le monde peut accéder aux objets présents dans le compartiment.
Tout le monde (accès public) : ACL	`READ_ACP`	Elles accordent un accès public en lecture pour l'ACL de compartiment. Lorsque vous accordez l'accès en lecture à Tout le monde (accès public), quiconque dans le monde peut accéder à l'ACL de compartiment.

Autorisation de la console	Autorisation de liste ACL	Accès
de compartiment – Lecture		

Pour plus d'informations sur les autorisations ACL, consultez Présentation de la liste de contrôle d'accès (ACL).

> **Important**
>
> Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Pour définir des autorisations de listes ACL pour un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste Compartiments, choisissez le nom du compartiment pour lequel vous souhaitez définir des autorisations.
4. Choisissez Permissions.
5. Sous Liste de contrôle d'accès, choisissez Modifier.

   Vous pouvez modifier les autorisations ACL suivantes pour le compartiment :

   Objets

   - List – Permet au bénéficiaire de lister les objets dans le compartiment.

- Write (Écriture) – Permet au bénéficiaire de créer des objets dans le compartiment. Pour les propriétaires de compartiments et d'objets existants, elles permettent également de supprimer et de remplacer ces objets.

  Dans la console S3, vous pouvez uniquement accorder un accès en écriture au groupe de mise à disposition de journaux S3 et au propriétaire du compartiment (le vôtre Compte AWS). Nous vous recommandons vivement de ne pas accorder l'accès en écriture aux autres bénéficiaires. Toutefois, si vous devez accorder un accès en écriture, vous pouvez utiliser l'API AWS CLI AWS SDKs, ou REST.

ACL du compartiment

- Read – Permet au bénéficiaire de lire la liste ACL du compartiment.
- Write – Permet au bénéficiaire d'écrire la liste ACL pour le compartiment applicable.

6. Pour modifier les autorisations du propriétaire du bucket, à côté du propriétaire du bucket (votre Compte AWS), effacez ou sélectionnez l'une des autorisations ACL suivantes :

   - Objets — Liste ou Écriture
   - ACL de compartiment — Lecture ou Écriture

   Le propriétaire fait référence à l'utilisateur Utilisateur racine d'un compte AWS, et non à un utilisateur AWS Identity and Access Management IAM. Pour plus d'informations sur l'utilisateur root, consultez Utilisateur racine d'un compte AWS dans le Guide de l'utilisateur IAM.

7. Pour octroyer ou annuler des autorisations pour le grand public (tout le monde sur Internet), en regard de Tout le monde (accès public), désactivez ou sélectionnez l'une des autorisations ACL suivantes :

   - Objets — Liste
   - ACL de compartiment — Lecture

   > **Warning**
   >
   > Soyez vigilant lorsque vous accordez au groupe Tout le monde l'accès public à votre compartiment S3. Lorsque vous accordez l'accès à ce groupe, tout le monde peut

accéder à votre compartiment. Nous vous recommandons vivement de ne jamais accorder un type d'accès en écriture public quel qu'il soit à votre compartiment S3.

8. Pour accorder ou annuler des autorisations à toute personne disposant d'un Compte AWSgroupe d'utilisateurs authentifiés (toute personne possédant un Compte AWS), effacez ou sélectionnez l'une des autorisations ACL suivantes :

   - Objets — Liste
   - ACL de compartiment — Lecture

9. Pour octroyer ou annuler des autorisations à Amazon S3 pour écrire des journaux d'accès au serveur dans le compartiment, sous Groupe de mise à disposition des journaux S3, désactivez ou sélectionnez l'une des autorisations ACL suivantes :

   - Objets — Liste ou Écriture
   - ACL de compartiment — Lecture ou Écriture

   Si un compartiment est configuré en tant que compartiment cible (les journaux d'accès y seront stockés), les autorisations sur ce compartiment doivent autoriser le groupe Livraison des journaux à disposer d'un accès en écriture sur le compartiment. Lorsque vous activez la journalisation des accès serveur sur un compartiment, la console Amazon S3 accorde au groupe Log Delivery (Livraison des journaux) un droit d'accès en écriture sur le compartiment que vous avez choisi pour la réception des journaux. Pour en savoir plus sur la journalisation des accès au serveur, consultez Activation de la journalisation des accès au serveur Amazon S3.

10. Pour accorder l'accès à une autre Compte AWS personne, procédez comme suit :

    a. Choisissez Ajouter un bénéficiaire.
    b. Dans la zone Bénéficiaire, saisissez l'ID canonique de l'autre Compte AWS.
    c. Sélectionnez l'une des autorisations ACL suivantes :

       - Objets — Liste ou Écriture
       - ACL de compartiment — Lecture ou Écriture

> ⚠ Warning
>
> Lorsque vous accordez à d'autres personnes l' Comptes AWS accès à vos ressources, sachez qu'elles Comptes AWS peuvent déléguer leurs autorisations aux utilisateurs de

leurs comptes. Il s'agit d'un accès intercompte. Pour en savoir plus sur l'utilisation de l'accès intercompte, consultez Création d'un rôle pour la délégation d'autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM.

11. Pour supprimer l'accès à un autre Compte AWS, sous Accès pour les autres Comptes AWS, choisissez Supprimer.
12. Sélectionnez Enregistrer pour enregistrer les modifications.

Utilisation de la console S3 pour définir des autorisations ACL pour un objet

La console affiche les autorisations d'accès combinées pour les bénéficiaires en double. Pour voir la liste complète des ACLs, utilisez l'API REST Amazon S3 AWS CLI, ou AWS SDKs. Le tableau suivant présente les autorisations ACL que vous pouvez configurer pour les objets dans la console Amazon S3.

Autorisations ACL de la console Amazon S3 pour les objets

Autorisation de la console	Autorisation de liste ACL	Accès
Objet – Lecture	`READ`	Elles permettent au bénéficiaire de lire les données de l'objet et ses métadonnées.
ACL de l'objet – Lecture	`READ_ACP`	Elles permettent au bénéficiaire de lire la liste ACL de l'objet.
ACL de l'objet – Écriture	`WRITE_ACP`	Elles permettent au bénéficiaire d'écrire la liste ACL pour l'objet applicable

Pour plus d'informations sur les autorisations ACL, consultez Présentation de la liste de contrôle d'accès (ACL).

Important

Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques

pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Pour définir des autorisations de liste ACL pour un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom du compartiment qui contient l'objet.
3. Dans la liste Objets, sélectionnez le nom de l'objet pour lequel vous souhaitez définir des autorisations.
4. Choisissez Permissions.
5. Sous Liste de contrôle d'accès (ACL), sélectionnez Modifier.

   Vous pouvez modifier les autorisations ACL suivantes pour l'objet :

   Objet

   - Read – Permet au bénéficiaire de lire les données de l'objet et ses métadonnées.

   Liste ACL de l'objet

   - Read – Permet au bénéficiaire de lire la liste ACL de l'objet.
   - Write – Permet au bénéficiaire d'écrire la liste ACL pour l'objet applicable. Dans la console S3, vous ne pouvez accorder l'accès en écriture qu'au propriétaire du compartiment (le vôtre Compte AWS). Nous vous recommandons vivement de ne pas accorder l'accès en écriture aux autres bénéficiaires. Toutefois, si vous devez accorder un accès en écriture, vous pouvez utiliser l'API AWS CLI AWS SDKs, ou REST.
6. Vous pouvez gérer les autorisations d'accès aux objets pour :

a. Accès pour le propriétaire de l'objet

   Le propriétaire fait référence à Utilisateur racine d'un compte AWS, et non à un utilisateur AWS Identity and Access Management IAM. Pour plus d'informations sur l'utilisateur root, consultez Utilisateur racine d'un compte AWS dans le Guide de l'utilisateur IAM.

   Pour modifier les autorisations d'accès aux objets du propriétaire, sous Accès pour le propriétaire de l'objet, sélectionnez Votre AWS compte (propriétaire).

   Activez les cases à cocher des autorisations que vous souhaitez modifier, puis choisissez Enregistrer.

b. Accès pour les autres Comptes AWS

   Pour accorder des autorisations à un autre AWS utilisateur Compte AWS, sous Accès pour les autres Comptes AWS, sélectionnez Ajouter un compte. Dans le champ Entrez un identifiant, entrez l'identifiant canonique de l' AWS utilisateur auquel vous souhaitez accorder des autorisations d'objets. Pour plus d'informations sur la recherche d'un identifiant canonique, consultez la section Vos Compte AWS identifiants dans le. Référence générale d'Amazon Web Services Vous pouvez ajouter jusqu'à 99 utilisateurs.

   Activez les cases à cocher des autorisations que vous souhaitez accorder à l'utilisateur, puis choisissez Enregistrer. Pour afficher des informations sur les autorisations, choisissez les icônes d'aide.

c. Accès public

   Pour permettre au grand public (tout le monde) d'accéder à votre objet, sous Accès public, sélectionnez Tout le monde. Si vous accordez des autorisations d'accès public, tout le monde peut accéder à l'objet.

   Activez les cases à cocher des autorisations que vous souhaitez accorder, puis choisissez Enregistrer.

   ⚠ Warning

   - Soyez vigilant lorsque vous accordez au groupe Everyone (Tout le monde) l'accès anonyme à vos objets Amazon S3. Lorsque vous accordez l'accès à ce groupe, tout le monde peut accéder à votre objet. Si vous avez besoin d'accorder l'accès

à tout le monde, nous vous recommandons vivement d'octroyer uniquement des autorisations Lecture d'objet.

- Nous vous recommandons de ne pas accorder des autorisations d'écriture sur l'objet au groupe Tout le monde. Si vous le faites, n'importe qui peut remplacer les autorisations de liste ACL pour l'objet.

À l'aide du AWS SDKs

Cette section fournit des exemples de configuration des attributions de liste ACL sur les compartiments et les objets.

> **Important**
>
> Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Java

Cette section fournit des exemples de configuration des attributions de liste ACL sur les compartiments et les objets. Le premier exemple crée un compartiment avec une liste ACL prête à l'emploi (voir Liste ACL prête à l'emploi), crée une liste personnalisée d'attributions d'autorisation, puis remplace l'ACL prête à l'emploi avec une ACL contenant les attributions personnalisées. Le second exemple montre comment modifier une ACL à l'aide de la méthode `AccessControlList.grantPermission()`.

Example Créer un compartiment et spécifier une liste ACL conservée qui octroie une autorisation au groupe de mise à disposition du journal S3

Cet exemple crée un compartiment. Dans le demande, l'exemple spécifie une liste ACL prête à l'emploi qui attribue au groupe Log Delivery l'autorisation d'écrire des journaux sur le compartiment.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.ArrayList;

public class CreateBucketWithACL {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String userEmailForReadPermission = "*** user@example.com ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .build();

            // Create a bucket with a canned ACL. This ACL will be replaced by the
            // setBucketAcl()
            // calls below. It is included here for demonstration purposes.
            CreateBucketRequest createBucketRequest = new
 CreateBucketRequest(bucketName, clientRegion.getName())
                    .withCannedAcl(CannedAccessControlList.LogDeliveryWrite);
            s3Client.createBucket(createBucketRequest);

            // Create a collection of grants to add to the bucket.
            ArrayList<Grant> grantCollection = new ArrayList<Grant>();

            // Grant the account owner full control.
            Grant grant1 = new Grant(new
 CanonicalGrantee(s3Client.getS3AccountOwner().getId()),
                    Permission.FullControl);
            grantCollection.add(grant1);

            // Grant the LogDelivery group permission to write to the bucket.
            Grant grant2 = new Grant(GroupGrantee.LogDelivery, Permission.Write);
            grantCollection.add(grant2);
```

```
            // Save grants by replacing all current ACL grants with the two we just
 created.
            AccessControlList bucketAcl = new AccessControlList();
            bucketAcl.grantAllPermissions(grantCollection.toArray(new Grant[0]));
            s3Client.setBucketAcl(bucketName, bucketAcl);

            // Retrieve the bucket's ACL, add another grant, and then save the new
 ACL.
            AccessControlList newBucketAcl = s3Client.getBucketAcl(bucketName);
            Grant grant3 = new Grant(new
 EmailAddressGrantee(userEmailForReadPermission), Permission.Read);
            newBucketAcl.grantAllPermissions(grant3);
            s3Client.setBucketAcl(bucketName, newBucketAcl);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example Mettre à jour la liste ACL sur un objet existant

L'exemple met à jour l'ACL sur un objet. L'exemple exécute les tâches suivantes :

- Extrait l'ACL d'un objet
- Efface la liste ACL en supprimant toutes les autorisations existantes
- Ajoute deux autorisations : plein accès au propriétaire, et WRITE_ACP (voir Quelles autorisations puis-je octroyer ?) à un utilisateur identifié par une adresse e-mail
- Enregistre l'ACL sur l'objet

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
```

```
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.AccessControlList;
import com.amazonaws.services.s3.model.CanonicalGrantee;
import com.amazonaws.services.s3.model.EmailAddressGrantee;
import com.amazonaws.services.s3.model.Permission;

import java.io.IOException;

public class ModifyACLExistingObject {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String emailGrantee = "*** user@example.com ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Get the existing object ACL that we want to modify.
            AccessControlList acl = s3Client.getObjectAcl(bucketName, keyName);

            // Clear the existing list of grants.
            acl.getGrantsAsList().clear();

            // Grant a sample set of permissions, using the existing ACL owner for
 Full
            // Control permissions.
            acl.grantPermission(new CanonicalGrantee(acl.getOwner().getId()),
 Permission.FullControl);
            acl.grantPermission(new EmailAddressGrantee(emailGrantee),
 Permission.WriteAcp);

            // Save the modified ACL back to the object.
            s3Client.setObjectAcl(bucketName, keyName, acl);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
```

```
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Example Créer un compartiment et spécifier une liste ACL conservée qui octroie une autorisation au groupe de mise à disposition du journal S3

Cet exemple C# crée un compartiment. Dans le demande, le code spécifie aussi une liste ACL prête à l'emploi qui attribue au groupe Log Delivery l'autorisation d'écrire les journaux sur le compartiment.

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingBucketACLTest
    {
        private const string newBucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            CreateBucketUseCannedACLAsync().Wait();
```

```
        }

        private static async Task CreateBucketUseCannedACLAsync()
        {
            try
            {
                // Add bucket (specify canned ACL).
                PutBucketRequest putBucketRequest = new PutBucketRequest()
                {
                    BucketName = newBucketName,
                    BucketRegion = S3Region.EUW1, // S3Region.US,
                                                  // Add canned ACL.
                    CannedACL = S3CannedACL.LogDeliveryWrite
                };
                PutBucketResponse putBucketResponse = await
 client.PutBucketAsync(putBucketRequest);

                // Retrieve bucket ACL.
                GetACLResponse getACLResponse = await client.GetACLAsync(new
 GetACLRequest
                {
                    BucketName = newBucketName
                });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("S3 error occurred. Exception: " +
 amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
}
```

Example Mettre à jour la liste ACL sur un objet existant

L'exemple C# met à jour l'ACL sur un objet existant. L'exemple exécute les tâches suivantes :

- Extrait l'ACL d'un objet.
- Efface la liste ACL en supprimant toutes les autorisations existantes.

- Ajoute deux autorisations : plein accès au propriétaire, et WRITE_ACP à un utilisateur identifié par une adresse e-mail.
- Enregistre l'ACL en envoyant une demande `PutAcl`.

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ManagingObjectACLTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** object key name ***";
        private const string emailAddress = "*** email address ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            TestObjectACLTestAsync().Wait();
        }
        private static async Task TestObjectACLTestAsync()
        {
            try
            {
                    // Retrieve the ACL for the object.
                    GetACLResponse aclResponse = await client.GetACLAsync(new
 GetACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName
                    });
```

```
                    S3AccessControlList acl = aclResponse.AccessControlList;

                    // Retrieve the owner (we use this to re-add permissions after
we clear the ACL).
                    Owner owner = acl.Owner;

                    // Clear existing grants.
                    acl.Grants.Clear();

                    // Add a grant to reset the owner's full permission (the
previous clear statement removed all permissions).
                    S3Grant fullControlGrant = new S3Grant
                    {
                        Grantee = new S3Grantee { CanonicalUser = owner.Id },
                        Permission = S3Permission.FULL_CONTROL

                    };

                    // Describe the grant for the permission using an email address.
                    S3Grant grantUsingEmail = new S3Grant
                    {
                        Grantee = new S3Grantee { EmailAddress = emailAddress },
                        Permission = S3Permission.WRITE_ACP
                    };
                    acl.Grants.AddRange(new List<S3Grant> { fullControlGrant,
grantUsingEmail });

                    // Set a new ACL.
                    PutACLResponse response = await client.PutACLAsync(new
PutACLRequest
                    {
                        BucketName = bucketName,
                        Key = keyName,
                        AccessControlList = acl
                    });
            }
            catch (AmazonS3Exception amazonS3Exception)
            {
                Console.WriteLine("An AmazonS3Exception was thrown. Exception: " +
amazonS3Exception.ToString());
            }
            catch (Exception e)
            {
```

```
                Console.WriteLine("Exception: " + e.ToString());
            }
        }
    }
}
```

Utilisation de l'API REST

Amazon S3 vous APIs permet de définir une ACL lorsque vous créez un bucket ou un objet. Amazon S3 fournit une API pour configurer une liste ACL sur un compartiment ou un objet existant. Elles APIs fournissent les méthodes suivantes pour définir une ACL :

- Configurer la liste ACL grâce aux en-têtes de demande – Lorsque vous envoyez une demande pour créer une ressource (compartiment ou objet), vous configurez une liste ACL grâce aux en-têtes de demande. Grâce à ces en-têtes, vous pouvez spécifier une liste ACL prête à l'emploi ou des accords (en identifiant explicitement le bénéficiaire et les autorisations).
- Configurer la liste ACL grâce au corps de la demande – Lorsque vous envoyez une demande pour configurer une liste ACL sur une ressource existante, vous pouvez configurer la liste ACL dans l'en-tête ou le corps de la demande.

Pour plus d'informations sur la prise en charge de la gestion par l'API REST ACLs, consultez les sections suivantes du manuel Amazon Simple Storage Service API Reference :

- GetBucketAcl
- PutBucketAcl
- GetObjecAcl
- PutObjectAcl
- PutObject
- CreateBucket
- CopyObject
- CreateMultipartUpload

> **Important**
>
> Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

En-têtes de demande spécifiques à une liste de contrôle d'accès (ACL)

Vous pouvez utiliser des en-têtes pour accorder des autorisations basées sur la liste de contrôle d'accès (ACL). Par défaut, tous les objets sont privés. Seul le propriétaire dispose d'un contrôle d'accès complet. Lorsque vous ajoutez un nouvel objet, vous pouvez accorder des autorisations à des individus Comptes AWS ou à des groupes prédéfinis définis par Amazon S3. Ces autorisations sont ensuite ajoutées à la liste de contrôle d'accès (ACL) sur l'objet. Pour plus d'informations, consultez Présentation de la liste de contrôle d'accès (ACL).

Avec cette opération, vous pouvez accorder des autorisations d'accès en utilisant l'une des deux méthodes suivantes :

- ACL prédéfini (**`x-amz-acl`**) : Amazon S3 prend en charge un ensemble de paramètres prédéfinis ACLs, appelés « scannés ACLs ». Chaque liste ACL prête à l'emploi possède un ensemble prédéfini de bénéficiaires et d'autorisations. Pour de plus amples informations, veuillez consulter Liste ACL prête à l'emploi.
- Autorisations d'accès — Pour accorder explicitement des autorisations d'accès à des groupes Comptes AWS ou à des groupes spécifiques, utilisez les en-têtes suivants. Chaque en-tête correspond à des autorisations spécifiques prises en charge par Amazon S3 dans une liste ACL. Pour plus d'informations, consultez Présentation de la liste de contrôle d'accès (ACL). Dans l'en-tête, vous spécifiez une liste de bénéficiaires qui obtiennent l'autorisation spécifique.
  - x-amz-grant-read
  - x-amz-grant-write
  - x-amz-grant-read-acp
  - x-amz-grant-write-acp
  - x-amz-grant-full-contrôle

En utilisant le AWS CLI

Pour plus d'informations sur la gestion de l' ACLs utilisation du AWS CLI, voir put-bucket-acllla référence des AWS CLI commandes.

> **Important**
>
> Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Exemples de politiques pour ACLs

Vous pouvez utiliser des clés de condition dans les politiques de compartiment pour contrôler l'accès à Amazon S3.

Rubriques

- Octroi de s3 : PutObject autorisation assortie d'une condition obligeant le propriétaire du bucket à obtenir le contrôle total
- Octroi de s3 : PutObject autorisation avec une condition sur l' x-amz-aclen-tête

Octroi de s3 : PutObject autorisation assortie d'une condition obligeant le propriétaire du bucket à obtenir le contrôle total

L'opération PUT Object autorise les en-têtes spécifiques à la liste de contrôle d'accès (ACL) que vous pouvez utiliser pour accorder des autorisations basées sur les listes ACL. En utilisant ces clés, le propriétaire du compartiment peut définir une condition pour nécessiter des autorisations d'accès spécifiques quand l'utilisateur charge un objet.

Supposons que le Compte A possède un compartiment et que l'administrateur du compte souhaite accorder à Dave, un utilisateur du Compte B, des autorisations pour charger des objets. Par défaut, les objets que Dave charge appartiennent au Compte B et le Compte A n'a aucune autorisation sur

ces objets. Le propriétaire du compartiment payant les factures, il souhaite toutes les autorisations sur les objets que Dave charge. L'administrateur du Compte A peut accomplir cela en octroyant l'autorisation `s3:PutObject` à Dave, avec une condition que la demande inclue des en-têtes spécifiques à la liste ACL, qui soit accorde explicitement une autorisation complète, soit utilise une liste ACL prédéfinie. Pour plus d'informations, consultez Objet PUT.

Exiger l' x-amz-full-controlen-tête

Vous pouvez exiger l'en-tête `x-amz-full-control` dans la demande avec une autorisation de contrôle total pour le propriétaire du compartiment. La politique de compartiment suivante octroie l'autorisation `s3:PutObject` à l'utilisateur Dave avec une condition utilisant la clé de condition `s3:x-amz-grant-full-control`, qui nécessite que la demande inclut l'en-tête `x-amz-full-control`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/Dave"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        }
    ]
}
```

> **Note**
>
> Cet exemple porte sur l'autorisation entre comptes. Toutefois, si Dave (qui obtient l'autorisation) appartient au propriétaire du Compte AWS bucket, cette autorisation

conditionnelle n'est pas nécessaire. En effet, le compte parent auquel Dave appartient possède des objets que l'utilisateur charge.

Ajouter un refus explicite

La politique de compartiment précédente octroie l'autorisation conditionnelle à l'utilisateur Dave du compte B. Tandis que cette stratégie est appliquée, il est possible pour Dave d'obtenir la même autorisation sans aucune condition par le biais d'autres stratégies. Par exemple, Dave peut appartenir à un groupe et vous octroyez l'autorisation `s3:PutObject` de groupe sans aucune condition. Pour éviter de telles failles d'autorisation, vous pouvez écrire une stratégie d'accès plus stricte en ajoutant un refus explicite. Dans cet exemple, vous refusez explicitement à l'utilisateur Dave l'autorisation de chargement s'il n'inclut pas les en-têtes nécessaires dans la demande octroyant des autorisations complète au propriétaire du compartiment. Le refus explicite a toujours priorité sur n'importe quelle autre autorisation accordée. Vous trouverez, ci-après, l'exemple révisé de stratégie d'accès avec un refus explicite ajouté.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        },
        {
            "Sid": "statement2",
            "Effect": "Deny",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::111122223333:user/AccountBadmin"
            },
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::awsexamplebucket1/*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-grant-full-control": "id=AccountA-CanonicalUserID"
                }
            }
        }
    ]
}
```

Testez la politique à l'aide du AWS CLI

Si vous en avez deux Comptes AWS, vous pouvez tester la politique à l'aide du AWS Command Line Interface (AWS CLI). Vous joignez la politique et utilisez les informations d'identification de Dave pour tester l'autorisation à l'aide de la AWS CLI `put-object` commande suivante. Vous fournissez les informations d'identification de Dave en ajoutant le paramètre `--profile`. Vous octroyez l'autorisation de contrôle complet au propriétaire du compartiment en ajoutant le paramètre `--grant-full-control`. Pour plus d'informations sur la configuration et l'utilisation du AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --grant-full-control id="AccountA-CanonicalUserID" --profile AccountBUserProfile
```

Exiger l' x-amz-aclen-tête

Vous pouvez exiger l'en-tête `x-amz-acl` avec une liste ACL prédéfinie octroyant une autorisation de contrôle complet au propriétaire du compartiment. Pour demander l'en-tête `x-amz-acl` dans la demande, vous pouvez remplacer la paire de clé-valeur dans le bloc `Condition` et spécifier la clé de condition `s3:x-amz-acl` comme indiqué dans l'exemple suivant.

```
"Condition": {
    "StringEquals": {
        "s3:x-amz-acl": "bucket-owner-full-control"
    }
}
```

Pour tester l'autorisation à l'aide du AWS CLI, vous devez spécifier le `--acl` paramètre. Il ajoute AWS CLI ensuite l'`x-amz-acl`en-tête lorsqu'il envoie la demande.

```
aws s3api put-object --bucket examplebucket --key HappyFace.jpg --body c:\HappyFace.jpg
 --acl "bucket-owner-full-control" --profile AccountBadmin
```

Octroi de s3 : PutObject autorisation avec une condition sur l' x-amz-acl en-tête

La politique de compartiment suivante accorde l'`s3:PutObject`autorisation à deux personnes Comptes AWS si la demande inclut l'`x-amz-acl`en-tête rendant l'objet lisible par le public. Le bloc `Condition` utilise la condition `StringEquals` et elle dispose d'une paire de clé-valeur, `"s3:x-amz-acl":["public-read"]`, pour évaluation. Dans la paire de clé-valeur, `s3:x-amz-acl` est une clé propre à Amazon S3, comme indiqué par le préfixe `s3:`.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AddCannedAcl",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:root",
                    "arn:aws:iam::111122223333:root"
                ]
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::awsexamplebucket1/*"
            ],
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": [
                        "public-read"
                    ]
                }
            }
        }
    ]
```

```
}
```

> **Important**
>
> Les conditions ne sont pas toutes logiques pour toutes les actions. Par exemple, il est logique d'inclure une condition `s3:LocationConstraint` sur une stratégie qui octroie l'autorisation Amazon S3 `s3:CreateBucket`. Cependant, il n'est pas logique d'inclure cette condition dans une politique qui accorde l'autorisation `s3:GetObject`. Amazon S3 peut rechercher les erreurs sémantiques pour ce type qui impliquent des conditions spécifiques à Amazon S3. Cependant, si vous créez une stratégie pour un rôle ou un utilisateur IAM et que vous incluez une condition Amazon S3 non valide sémantiquement, aucune erreur n'est rapportée car IAM ne peut pas valider les conditions Amazon S3.

Blocage de l'accès public à votre stockage Amazon S3

La fonction du blocage de l'accès public Amazon S3 fournit des paramètres pour les points d'accès, les compartiments et les comptes afin de vous aider à gérer l'accès public aux ressources Amazon S3. Par défaut, les nouveaux compartiments, points d'accès et objets n'autorisent pas l'accès public. Toutefois, les utilisateurs peuvent modifier les stratégies de compartiment, les stratégies de point d'accès ou les autorisations d'objet pour autoriser l'accès public. Les paramètres de la fonctionnalité de blocage de l'accès public S3 remplacent ces stratégies et autorisations pour que vous puissiez restreindre l'accès public à ces ressources.

Grâce au blocage de l'accès public Amazon S3, les administrateurs de compte et les propriétaires de compartiment configurent facilement les contrôles centralisés, afin de restreindre l'accès public à leurs ressources Amazon S3. Ces contrôles sont appliqués quel que soit le mode de création de ces ressources.

Pour obtenir des instructions sur la configuration du blocage de l'accès public, consultez Configuration du blocage d'accès public.

Quand Amazon S3 reçoit une demande d'accès à un compartiment ou à un objet, il détermine si le paramètre de blocage de l'accès public est défini pour le compartiment ou le compte du propriétaire de compartiment. Si la demande a été effectuée via un point d'accès, Amazon S3 vérifie également les paramètres de blocage de l'accès public pour le point d'accès. S'il existe un paramètre de blocage de l'accès public interdisant l'accès demandé, Amazon S3 rejette la demande.

Le blocage de l'accès public Amazon S3 fournit quatre paramètres. Ces paramètres sont indépendants et peuvent être fournis sous n'importe quelle combinaison. Chaque paramètre peut être appliqué à un point d'accès, à un compartiment ou à un Compte AWS entier. Si les paramètres de blocage de l'accès public pour le point d'accès, le compartiment ou le compte diffèrent, Amazon S3 applique la combinaison la plus restrictive des paramètres du point d'accès, du compartiment et du compte.

Quand Amazon S3 évalue si une opération est interdite par un paramètre de blocage de l'accès public, il rejette toute demande qui irait à l'encontre d'un paramètre de point d'accès, de compartiment ou de compte.

Important

L'accès public est accordé aux compartiments et aux objets par le biais de listes de contrôle d'accès (ACLs), de politiques de point d'accès, de politiques de compartiments, ou de toutes les politiques. Pour être sûr que l'accès public à tous vos points d'accès, compartiments et objets Amazon S3 est bloqué, nous vous recommandons d'activer les quatre paramètres liés au blocage de l'accès public pour votre compte. Ces paramètres bloquent l'accès public pour tous les compartiments et points d'accès présents et futurs.
Avant d'appliquer ces paramètres, vérifiez que vos applications fonctionnent correctement sans accès public. Si vous avez besoin d'un certain niveau d'accès public à vos compartiments ou objets, par exemple pour héberger un site web statique comme décrit dans Hébergement d'un site Web statique à l'aide d'Amazon S3, vous pouvez personnaliser les paramètres individuels afin de les adapter à vos cas d'utilisation du stockage.
L'activation du blocage de l'accès public permet de protéger vos ressources en empêchant l'accès public d'être accordé par le biais des politiques de ressources ou des listes de contrôle d'accès (ACLs) directement associées aux ressources S3. Outre l'activation du blocage de l'accès public, examinez attentivement les politiques suivantes pour vous assurer qu'elles n'accordent pas l'accès public :

- Politiques basées sur l'identité associées aux AWS principaux associés (par exemple, les rôles IAM)
- Politiques basées sur les AWS ressources associées (par exemple, clés AWS Key Management Service (KMS))

> **Note**
>
> - Vous pouvez activer les paramètres de blocage de l'accès public uniquement pour les points d'accès, les compartiments et les Comptes AWS. Amazon S3 ne prend pas en charge les paramètres de blocage de l'accès public par objet.
> - Lorsque vous appliquez des paramètres de blocage de l'accès public à un compte, ils s'appliquent à tous Régions AWS dans le monde entier. Les paramètres peuvent ne pas prendre effet immédiatement ou simultanément dans toutes les Régions, mais ils finissent par s'y propager.

Rubriques

- Paramètres de la fonctionnalité de blocage de l'accès public
- Exécution d'opérations de blocage d'accès public sur un point d'accès
- La signification du mot « public »
- Utilisation de l'analyseur d'accès IAM pour S3 pour passer en revue les compartiments publics
- Autorisations
- Configuration du blocage d'accès public
- Configuration des paramètres de blocage d'accès public pour votre compte
- Configuration des paramètres de blocage d'accès public pour vos compartiments S3

Paramètres de la fonctionnalité de blocage de l'accès public

La fonctionnalité de blocage de l'accès public S3 fournit quatre paramètres. Vous pouvez appliquer ces paramètres de manière combinée à des points d'accès, à des compartiments ou à des Comptes AWS entiers. Si vous appliquez un paramètre à un compte, il s'applique à tous les compartiments et points d'accès appartenant à ce compte. De même, si vous appliquez un paramètre à un compartiment, il s'applique à tous les points d'accès associés à ce compartiment.

Le tableau suivant contient les paramètres disponibles.

Nom	Description
`BlockPublicAcls`	La configuration de cette option sur `TRUE` entraîne le comportement suivant :

Nom	Description
	• Les appels `PutBucketAcl` et `PutObjectAcl` échouent si la liste de contrôle d'accès (ACL) spécifiée est publique. • Les appels `PutObject` échouent si la demande inclut une ACL publique. • Si ce paramètre est appliqué à un compte, les `PUT Bucket` appels échouent si la demande inclut une ACL publique. Lorsque ce paramètre est défini sur`TRUE`, les opérations spécifiées échouent (qu'elles soient effectuées via l'API REST ou AWS SDKs). AWS CLI Toutefois, les politiques existantes et celles ACLs relatives aux compartiments et aux objets ne sont pas modifiées. Ce paramètre vous permet de vous protéger contre l'accès public tout en vous permettant d'auditer, d'affiner ou de modifier les politiques existantes ainsi que celles ACLs relatives à vos compartiments et objets. **Note** Les points d'accès ne leur sont pas ACLs associés. Si vous appliquez ce paramètre à un point d'accès, il agit comme une transmission au compartiment sous-jacent. Si ce paramètre est activé sur un point d'accès, les demandes effectuées via le point d'accès se comportent comme si ce paramètre était activé dans le compartiment sous-jacent, que ce paramètre soit activé ou non dans le compartiment.

Nom	Description
`IgnorePublicAcls`	Si cette option est définie`TRUE`, Amazon S3 ignore tous les éléments publics ACLs d'un compartiment et tous les objets qu'il contient. Ce paramètre vous permet de bloquer en toute sécurité l'accès public accordé par ACLs tout en autorisant les `PutObject` appels qui incluent une ACL publique (par opposition à ceux `BlockPublicAcls` qui rejettent les `PutObject` appels qui incluent une ACL publique). L'activation de ce paramètre n'affecte pas la persistance des paramètres existants ACLs et n'empêche pas la définition d'un nouveau public ACLs . **Note** Les points d'accès ne leur sont pas ACLs associés. Si vous appliquez ce paramètre à un point d'accès, il agit comme une transmission au compartiment sous-jacent. Si ce paramètre est activé sur un point d'accès, les demandes effectuées via le point d'accès se comportent comme si ce paramètre était activé dans le compartiment sous-jacent, que ce paramètre soit activé ou non dans le compartiment.

Nom	Description
`BlockPublicPolicy`	Si cette option est définie sur `TRUE` pour un compartiment, Amazon S3 rejette les appels `PutBucketPolicy` si la politique de compartiment spécifiée autorise l'accès public. Si cette option est définie sur `TRUE` pour un compartiment, Amazon S3 rejette également les appels `PutAccessPointPolicy` destinés à tous les points d'accès du même compte du compartiment si la politique spécifiée autorise l'accès public. Si cette option est définie sur « `TRUE` pour un point d'accès », Amazon S3 rejette `PutBucketPolicy` les appels vers `PutAccessPointPolicy` et passés par le point d'accès si la politique spécifiée (pour le point d'accès ou le compartiment sous-jacent) autorise l'accès public. Vous pouvez utiliser ce paramètre pour autoriser les utilisateurs à gérer des stratégies de point d'accès et de compartiment, sans toutefois les autoriser à partager publiquement le compartiment ou les objets qu'il contient. L'activation de ce paramètre n'a pas d'incidence sur les stratégies de point d'accès ou de compartiment existantes. **Important** Pour utiliser ce paramètre efficacement, nous vous recommandons de l'appliquer au niveau du compte. Une politique de compartiment peut autoriser les utilisateurs à modifier les paramètres de blocage de l'accès public d'un compte. Par conséquent, les utilisateurs autorisés à modifier une politique de compartiment peuvent insérer une stratégie qui leur permet de désactiver les paramètres de blocage de l'accès public pour le compartiment. Si ce paramètre est activé pour le compte entier, et non pour un compartiment spécifique, Amazon S3 bloque les stratégies publiques même si un utilisateur modifie la politique de compartiment pour désactiver ce paramètre.

Nom	Description
`RestrictPublicBuckets`	Si vous définissez cette option de `TRUE` manière à restreindre l'accès à un point d'accès ou à un bucket soumis à une politique publique, aux seuls responsables du AWS service et aux utilisateurs autorisés du compte du propriétaire du bucket et du compte du propriétaire du point d'accès. Ce paramètre bloque tous les accès entre comptes au point d'accès ou au compartiment (sauf pour les responsables du AWS service), tout en permettant aux utilisateurs du compte de gérer le point d'accès ou le compartiment. L'activation de ce paramètre n'a pas d'incidence sur les stratégies de point d'accès ou de compartiment existantes, mais Amazon S3 bloque l'accès public et entre comptes provenant des stratégies de point d'accès ou de compartiment publiques, notamment la délégation non publique à des comptes spécifiques.

Important

- Appelle `GetBucketAcl` et renvoie `GetObjectAcl` toujours les autorisations effectives en place pour le bucket ou l'objet spécifié. Par exemple, supposons qu'un compartiment dispose d'une ACL accordant l'accès public, mais que le paramètre `IgnorePublicAcls` soit également activé pour le même compartiment. Dans ce cas, `GetBucketAcl` renvoie une ACL qui reflète les autorisations d'accès appliquées par Amazon S3, plutôt que l'ACL réelle associée au bucket.
- Les paramètres de blocage de l'accès public ne modifient pas les politiques existantes ou ACLs. Par conséquent, la suppression d'un paramètre de blocage de l'accès public conduit un compartiment ou un objet doté d'une ACL ou d'une stratégie publique à de nouveau être accessible publiquement.

Exécution d'opérations de blocage d'accès public sur un point d'accès

Pour effectuer des opérations de blocage de l'accès public sur un point d'accès, utilisez le AWS CLI services`s3control`.

> **Important**
>
> Vous ne pouvez pas modifier les paramètres de blocage de l'accès public d'un point d'accès après avoir créé le point d'accès. Vous pouvez spécifier les paramètres de blocage de l'accès public pour un point d'accès uniquement lors de la création du point d'accès.

La signification du mot « public »

ACLs

Amazon S3 considère qu'une ACL de compartiment ou d'objet est publique si elle accorde des autorisations aux membres des groupes `AllUsers` ou `AuthenticatedUsers` prédéfinis. Pour plus d'informations sur les groupes prédéfinis, consultez Groupes prédéfinis Amazon S3.

Politiques de compartiment

Lors de l'évaluation d'une politique de compartiment, Amazon S3 commence par assumer que la stratégie est publique. Puis, il évalue la stratégie pour déterminer si elle qualifiée comme non publique. Pour être considérée comme non publique, une politique de compartiment doit accorder l'accès uniquement aux valeurs fixes (valeurs ne contenant aucun caractère générique ni aucune variable de politique AWS Identity and Access Management) d'un ou de plusieurs des éléments suivants :

- Un AWS principal, un utilisateur, un rôle ou un responsable de service (par exemple`aws:PrincipalOrgID`)
- Un ensemble de blocs de routage interdomaines sans classe (CIDR), utilisant. `aws:SourceIp` Pour plus d'informations sur CIDR, consultez RFC 4632 sur le site web RFC Editor.

> **Note**
>
> Les politiques de compartiment qui accordent un accès conditionné par la clé de condition `aws:SourceIp` avec de très larges plages d'adresses IP (par exemple, 0.0.0.0/1) sont considérées comme « publiques ». Cela inclut des valeurs plus larges que `/8` pour IPv4 et `/32` pour IPv6 (à l'exception des plages RFC1918 privées). Bloquer l'accès public rejettera ces politiques « publiques » et empêchera l'accès entre comptes aux compartiments qui utilisent déjà ces politiques « publiques ».

- `aws:SourceArn`
- `aws:SourceVpc`
- `aws:SourceVpce`
- `aws:SourceOwner`
- `aws:SourceAccount`
- `aws:userid`, hors du modèle `"AROLEID:*"`
- `s3:DataAccessPointArn`

> **Note**
>
> Lorsqu'elle est utilisée dans une politique de compartiment, cette valeur peut contenir un caractère générique pour le nom du point d'accès sans rendre la politique publique, à condition que l'identifiant du compte soit fixe. Par exemple, autoriser l'accès à `arn:aws:s3:us-west-2:123456789012:accesspoint/*` permettrait l'accès à n'importe quel point d'accès associé au compte `123456789012` dans la Région `us-west-2`, sans rendre la politique de compartiment publique. Ce comportement est différent pour les politiques de point d'accès. Pour de plus amples informations, veuillez consulter Points d'accès.

- `s3:DataAccessPointAccount`

Pour plus d'informations sur les stratégies de compartiment, consultez Politiques de compartiment pour Amazon S3.

> **Note**
>
> Lorsque vous utilisez des clés de contexte à valeurs multiples, vous devez utiliser les opérateurs `ForAllValues` ou `ForAnyValue` set.

Example : politiques relatives aux compartiments publics

Conformément à ces règles, les exemples de stratégies suivants sont considérés comme publics.

```
{
  "Principal": "*",
  "Resource": "*",
```

```
  "Action": "s3:PutObject",
  "Effect": "Allow"
 }
```

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": { "StringLike": {"aws:SourceVpc": "vpc-*"}}
 }
```

Ces stratégies peuvent devenir non publiques grâce à une valeur fixe en incluant l'une des clés de condition énumérée précédemment. Par exemple, la dernière stratégie ci-dessus peut devenir non publique si vous définissez `aws:SourceVpc` sur une valeur fixe, comme suit :

```
{
  "Principal": "*",
  "Resource": "*",
  "Action": "s3:PutObject",
  "Effect": "Allow",
  "Condition": {"StringEquals": {"aws:SourceVpc": "vpc-91237329"}}
 }
```

Comment Amazon S3 évalue une politique de compartiment qui contient des autorisations d'accès publiques et non publiques ?

Cet exemple illustre comment Amazon S3 évalue une politique de compartiment contenant des autorisations d'accès publiques et non publiques.

Supposons qu'un compartiment dispose d'une stratégie qui accorde l'accès à un ensemble de mandataires fixes. Conformément aux règles précédemment décrites, cette stratégie n'est pas publique. Ainsi, si vous activez le paramètre `RestrictPublicBuckets`, la stratégie reste effective comme indiqué, car `RestrictPublicBuckets` s'applique uniquement aux compartiments disposant de stratégies publiques. Cependant, si vous ajoutez une déclaration publique à la stratégie, `RestrictPublicBuckets` s'applique au compartiment. Il permet uniquement aux responsables du AWS service et aux utilisateurs autorisés du compte du propriétaire du bucket d'accéder au bucket.

Par exemple, supposons qu'un compartiment détenu par « Account-1 » dispose d'une stratégie contenant les éléments suivants :

1. Une déclaration qui accorde l'accès à AWS CloudTrail (qui est un principal AWS de service)
2. Une instruction qui accorde l'accès au compte « Account-2 »
3. Une instruction qui accorde l'accès au public, par exemple en indiquant `"Principal": "*"` sans aucune `Condition` restrictive

Cette stratégie peut être publique à cause de la troisième instruction. Une fois cette politique en place et `RestrictPublicBuckets` activée, Amazon S3 autorise l'accès uniquement par CloudTrail. Notez que bien que l'instruction 2 ne soit pas publique, Amazon S3 désactive l'accès à « Account-2 ». En effet, l'instruction 3 permet à la stratégie entière de devenir publique, ainsi `RestrictPublicBuckets` s'applique. Par conséquent, Amazon S3 désactive l'accès intercompte, bien que la stratégie délègue l'accès à un compte spécifique, « Account-2 ». Mais si vous supprimez l'instruction 3 de la stratégie, cette dernière ne peut pas être publique et `RestrictPublicBuckets` ne s'applique plus. Ainsi, « Account-2 » a de nouveau accès au compartiment, même si `RestrictPublicBuckets` reste activé.

Points d'accès

Amazon S3 évalue les paramètres de blocage de l'accès public de façon légèrement différente pour les points d'accès par rapport aux compartiments. Les règles qu'Amazon S3 applique pour déterminer quand une stratégie de point d'accès est publique sont généralement les mêmes pour les points d'accès et pour les compartiments, sauf dans les cas suivants :

- Un point d'accès ayant une origine réseau VPC est toujours considéré comme non public, quel que soit le contenu de sa stratégie de point d'accès.
- Une stratégie de point d'accès qui accorde l'accès à un ensemble de points d'accès utilisant `s3:DataAccessPointArn` est considérée comme publique. Notez que ce comportement est différent de celui des stratégies de compartiment. Par exemple, une politique de compartiment qui accorde l'accès aux valeurs de `s3:DataAccessPointArn` correspondant à `arn:aws:s3:us-west-2:123456789012:accesspoint/*` n'est pas considérée comme publique. Toutefois, la même instruction dans une stratégie de point d'accès rendrait le point d'accès public.

Utilisation de l'analyseur d'accès IAM pour S3 pour passer en revue les compartiments publics

Vous pouvez utiliser IAM Access Analyzer pour S3 pour examiner les compartiments contenant des compartiments ACLs, des politiques de compartiment ou des politiques de point d'accès qui

accordent un accès public. IAM Access Analyzer for S3 vous avertit de la présence de compartiments configurés pour autoriser l'accès à toute personne sur Internet ou autre Comptes AWS, y compris Comptes AWS en dehors de votre organisation. Pour chaque compartiment public ou partagé, vous recevez des résultats qui signalent la source et le niveau d'accès public ou partagé.

Dans l'analyseur d'accès IAM pour S3, vous pouvez bloquer tout accès public à un compartiment en un seul clic. Vous pouvez également aller plus loin en configurant des niveaux d'accès précis dans les paramètres des niveaux d'autorisation des compartiments. Pour les cas d'utilisation spécifiques et vérifiés nécessitant un accès public ou partagé, vous pouvez confirmer et enregistrer votre intention de maintenir le niveau d'accès public ou partagé en archivant les résultats pour le compartiment.

Dans de rares cas, l'évaluation de l'accès public par bloc IAM Access Analyzer pour S3 et Amazon S3 peut différer selon qu'un bucket est public ou non. Ce comportement est dû au fait qu'Amazon S3 bloque l'accès public et valide l'existence d'actions en plus d'évaluer l'accès public. Supposons que la politique du compartiment contienne une `Action` déclaration qui autorise l'accès public pour une action qui n'est pas prise en charge par Amazon S3 (par exemple,`s3:NotASupportedAction`). Dans ce cas, le blocage de l'accès public par Amazon S3 considère le compartiment comme étant public, car une telle déclaration pourrait potentiellement le rendre public si l'action est prise en charge ultérieurement. Dans les cas où Amazon S3 bloque l'accès public et IAM Access Analyzer for S3 diffèrent dans leurs évaluations, nous vous recommandons de revoir la politique des compartiments et de supprimer toutes les actions non prises en charge.

Pour plus d'informations sur l'analyseur d'accès IAM pour S3, consultez Examen de l'accès aux compartiments à l'aide de l'analyseur d'accès IAM pour S3.

Autorisations

Pour utiliser les fonctions du blocage de l'accès public Amazon S3, vous devez disposer des autorisations suivantes.

Opération	Autorisations requises
`GET`État de la politique du bucket	`s3:GetBucketPolicyStatus`
`GET`Paramètres d'accès public du bucket Block	`s3:GetBucketPublicAccessBlock`
`PUT`Paramètres d'accès public du bucket Block	`s3:PutBucketPublicAccessBlock`

Opération	Autorisations requises
`DELETE`Paramètres d'accès public du bucket Block	`s3:PutBucketPublicAccessBlock`
`GET`paramètres de blocage de l'accès public au compte	`s3:GetAccountPublicAccessBlock`
`PUT`paramètres de blocage de l'accès public au compte	`s3:PutAccountPublicAccessBlock`
`DELETE`paramètres de blocage de l'accès public au compte	`s3:PutAccountPublicAccessBlock`
`PUT`paramètres du point d'accès Bloquer l'accès public	`s3:CreateAccessPoint`

> **Note**
>
> Les `DELETE` opérations nécessitent les mêmes autorisations que les `PUT` opérations. Il n'existe aucune autorisation distincte pour les `DELETE` opérations.

Configuration du blocage d’accès public

Pour plus d'informations sur la configuration de l'accès public par blocs pour vos Compte AWS compartiments Amazon S3 et vos points d'accès, consultez les rubriques suivantes :

- Configuration des paramètres de blocage d’accès public pour votre compte
- Configuration des paramètres de blocage d’accès public pour vos compartiments S3
- Exécution d’opérations de blocage d’accès public sur un point d’accès

Configuration des paramètres de blocage d’accès public pour votre compte

La fonction du blocage de l’accès public Amazon S3 fournit des paramètres pour les points d’accès, les compartiments et les comptes afin de vous aider à gérer l’accès public aux ressources

Amazon S3. Par défaut, les nouveaux compartiments, points d'accès et objets n'autorisent pas l'accès public.

Pour plus d'informations, consultez Blocage de l'accès public à votre stockage Amazon S3.

> **Note**
>
> Les paramètres au niveau du compte remplacent les paramètres sur les objets individuels. La configuration de votre compte pour bloquer l'accès public annulera tous les paramètres d'accès public définis pour les objets individuels de votre compte.

Vous pouvez utiliser la console S3, AWS CLI AWS SDKs, et l'API REST pour configurer les paramètres de blocage de l'accès public pour tous les compartiments de votre compte. Consultez les sections ci-dessous pour en savoir plus.

Pour configurer les paramètres de blocage d'accès public pour vos compartiments, consultez Configuration des paramètres de blocage d'accès public pour vos compartiments S3. Pour plus d'informations sur les points d'accès, consultez Exécution d'opérations de blocage d'accès public sur un point d'accès.

Utiliser la console S3.

La fonctionnalité de blocage de l'accès public Amazon S3 empêche l'application de paramètres qui autorisent un accès public aux données dans des compartiments S3. Cette section explique comment modifier les paramètres de blocage de l'accès public pour tous les compartiments S3 de votre Compte AWS. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

Pour modifier les paramètres de blocage de l'accès public pour tous les compartiments S3 d'un Compte AWS

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Block Public Access settings for this account (Bloquer les paramètres d'accès public pour ce compte).
3. Choisissez Edit (Modifier) pour modifier les paramètres de blocage de l'accès public pour tous les compartiments de votre Compte AWS.

4. Choisissez les paramètres que vous souhaitez modifier, puis Enregistrer.
5. Lorsque vous êtes invité à confirmer l'opération, entrez **`confirm`**. Choisissez ensuite Confirmer pour enregistrer vos modifications.

En utilisant le AWS CLI

Vous pouvez utiliser le blocage de l'accès public Amazon S3 via AWS CLI. Pour plus d'informations sur la configuration et l'utilisation du AWS CLI, voir Qu'est-ce que le AWS Command Line Interface ?

Compte

Pour effectuer des opérations Block Public Access sur un compte, utilisez le service AWS CLI de `s3control`. Les opérations au niveau des comptes qui utilisent ce service sont les suivantes :

- `PutPublicAccessBlock`(pour un compte)
- `GetPublicAccessBlock`(pour un compte)
- `DeletePublicAccessBlock`(pour un compte)

Pour des informations supplémentaires et des exemples, voir put-public-access-blockla AWS CLI référence.

À l'aide du AWS SDKs

Java

Les exemples suivants vous montrent comment utiliser Amazon S3 Block Public Access AWS SDK pour Java pour configurer un bloc d'accès public sur un compte Amazon S3.

```
AWSS3ControlClientBuilder controlClientBuilder =
 AWSS3ControlClientBuilder.standard();
controlClientBuilder.setRegion(<region>);
controlClientBuilder.setCredentials(<credentials>);

AWSS3Control client = controlClientBuilder.build();
client.putPublicAccessBlock(new PutPublicAccessBlockRequest()
  .withAccountId(<account-id>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withIgnorePublicAcls(<value>)
    .withBlockPublicAcls(<value>)
```

```
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

> **Important**
>
> Cet exemple s'applique uniquement aux opérations au niveau des comptes qui utilisent la classe client `AWSS3Control`. Pour les opérations au niveau des compartiments, consultez l'exemple précédent.

Other SDKs

Pour plus d'informations sur l'utilisation de l'autre AWS SDKs, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Utilisation de l'API REST

Pour plus d'informations sur l'utilisation d'Amazon S3 Block Public Access via REST APIs, consultez les rubriques suivantes dans le manuel Amazon Simple Storage Service API Reference.

- Opérations au niveau des comptes
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock

Configuration des paramètres de blocage d'accès public pour vos compartiments S3

La fonction du blocage de l'accès public Amazon S3 fournit des paramètres pour les points d'accès, les compartiments et les comptes afin de vous aider à gérer l'accès public aux ressources Amazon S3. Par défaut, les nouveaux compartiments, points d'accès et objets n'autorisent pas l'accès public.

Pour de plus amples informations, veuillez consulter Blocage de l'accès public à votre stockage Amazon S3.

Vous pouvez utiliser la console S3, AWS CLI AWS SDKs, et l'API REST pour accorder un accès public à un ou plusieurs compartiments. Vous pouvez également bloquer l'accès public à des compartiments qui sont déjà publics. Consultez les sections ci-dessous pour en savoir plus.

Pour configurer les paramètres de blocage de l'accès public pour chaque compartiment dans votre compte, consultez Configuration des paramètres de blocage d'accès public pour votre compte. Pour plus d'informations sur la configuration du blocage de l'accès public des points d'accès, consultez Exécution d'opérations de blocage d'accès public sur un point d'accès.

Utiliser la console S3.

La fonctionnalité de blocage de l'accès public Amazon S3 empêche l'application de paramètres qui autorisent un accès public aux données dans des compartiments S3. Cette section explique comment modifier les paramètres de la fonctionnalité de blocage de l'accès public pour un ou plusieurs compartiments S3. Pour plus d'informations sur le blocage de l'accès public à l'aide de AWS CLI AWS SDKs,, et du REST Amazon S3 APIs, consultezBlocage de l'accès public à votre stockage Amazon S3.

Vous pouvez voir si votre bucket est accessible au public dans la liste des buckets, dans la colonne IAM Access Analyzer. Pour de plus amples informations, veuillez consulter Examen de l'accès aux compartiments à l'aide de l'analyseur d'accès IAM pour S3.

Si vous voyez une `Error` lorsque vous répertoriez vos compartiments et leurs paramètres d'accès public, il se peut que vous ne disposiez pas des autorisations requises. Assurez-vous d'avoir ajouté les autorisations suivantes à votre politique d'utilisateur ou de rôle :

```
s3:GetAccountPublicAccessBlock
s3:GetBucketPublicAccessBlock
s3:GetBucketPolicyStatus
s3:GetBucketLocation
s3:GetBucketAcl
s3:ListAccessPoints
s3:ListAllMyBuckets
```

Dans de rares cas, les demandes peuvent également échouer en raison d'un Région AWS Pannes.

Pour modifier les paramètres de blocage de l'accès public Amazon S3 pour un compartiment S3 simple

Suivez ces étapes si vous devez modifier les paramètres d'accès public pour un seul compartiment S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment que vous souhaitez utiliser.
3. Choisissez Permissions.
4. Choisissez Modifier à côté de Bloquer l'accès public (paramètres du compartiment) pour modifier les paramètres d'accès public du compartiment. Pour en savoir plus sur les quatre paramètres de blocage de l'accès public Amazon S3, consultez Paramètres de la fonctionnalité de blocage de l'accès public.
5. Choisissez l'un des paramètres, puis cliquez sur Enregistrer les modifications.
6. Lorsque vous êtes invité à confirmer l'opération, entrez **`confirm`**. Choisissez ensuite Confirmer pour enregistrer vos modifications.

Vous pouvez également modifier les paramètres de blocage de l'accès public d'Amazon S3 lorsque vous créez un bucket. Pour de plus amples informations, veuillez consulter Création d'un bucket à usage général.

En utilisant le AWS CLI

Pour bloquer l'accès public à un bucket ou pour supprimer le blocage d'accès public, utilisez le AWS CLI services`s3api`. Les opérations au niveau des compartiments qui utilisent ce service sont les suivantes :

- `PutPublicAccessBlock`(pour un seau)
- `GetPublicAccessBlock`(pour un seau)
- `DeletePublicAccessBlock`(pour un seau)
- `GetBucketPolicyStatus`

Pour plus d'informations et des exemples, consultez put-public-access-block dans la référence AWS CLI .

À l'aide du AWS SDKs

Java

```
AmazonS3 client = AmazonS3ClientBuilder.standard()
   .withCredentials(<credentials>)
   .build();

client.setPublicAccessBlock(new SetPublicAccessBlockRequest()
  .withBucketName(<bucket-name>)
  .withPublicAccessBlockConfiguration(new PublicAccessBlockConfiguration()
    .withBlockPublicAcls(<value>)
    .withIgnorePublicAcls(<value>)
    .withBlockPublicPolicy(<value>)
    .withRestrictPublicBuckets(<value>)));
```

> **Important**
>
> Cet exemple s'applique uniquement aux opérations au niveau des compartiments qui utilisent la classe client `AmazonS3`. Pour les opérations au niveau des comptes, consultez l'exemple suivant.

Other SDKs

Pour plus d'informations sur l'utilisation de l'autre AWS SDKs, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Utilisation de l'API REST

Pour plus d'informations sur l'utilisation d'Amazon S3 Block Public Access via REST APIs, consultez les rubriques suivantes dans le manuel Amazon Simple Storage Service API Reference.

- Opérations au niveau des compartiments
  - PutPublicAccessBlock
  - GetPublicAccessBlock
  - DeletePublicAccessBlock
  - GetBucketPolicyStatus

Examen de l'accès aux compartiments à l'aide de l'analyseur d'accès IAM pour S3

IAM Access Analyzer pour S3 fournit des résultats d'accès externes pour vos compartiments S3 à usage général qui sont configurés pour autoriser l'accès à toute personne sur Internet (public) ou autre Comptes AWS, y compris Comptes AWS en dehors de votre organisation. Pour chaque compartiment partagé publiquement ou avec d'autres utilisateurs Comptes AWS, vous recevez des informations sur la source et le niveau d'accès partagé. Par exemple, l'analyseur d'accès IAM pour S3 peut montrer qu'un compartiment dispose d'un accès en lecture ou en écriture fourni via une liste de contrôle d'accès (ACL) de compartiment, une politique de compartiment, une politique de point d'accès multirégion ou une politique de point d'accès. Grâce à ces résultats, vous pouvez prendre des mesures correctives immédiates et précises pour rétablir l'accès à votre compartiment comme vous l'aviez prévu.

La console Amazon S3 présente un résumé des accès externes dans la console S3 à côté de votre liste de compartiments à usage général. Dans le résumé, vous pouvez cliquer sur les résultats actifs de chacun Région AWS pour voir les détails des résultats sur la page IAM Access Analyzer pour S3. Les résultats relatifs aux accès externes figurant dans le résumé des accès externes sont automatiquement mis à jour toutes les 24 heures.

Lorsque vous examinez un compartiment qui autorise l'accès public, sur la page IAM Access Analyzer pour S3, vous pouvez bloquer tout accès public au compartiment en un seul clic. Nous vous recommandons de bloquer tout accès public à vos buckets, sauf si vous avez besoin d'un accès public pour prendre en charge un cas d'utilisation spécifique. Avant de bloquer tout accès public, assurez-vous que vos applications continueront à fonctionner correctement sans accès public. Pour plus d'informations, consultez Blocage de l'accès public à votre stockage Amazon S3.

Vous pouvez également aller plus loin en configurant des niveaux d'accès précis dans les paramètres des niveaux d'autorisation des compartiments. Pour des cas d'utilisation spécifiques et vérifiés nécessitant un accès public, tels que l'hébergement statique de site web, les téléchargements publics ou le partage entre comptes, vous pouvez confirmer et enregistrer votre intention pour que le compartiment reste public ou partagé en archivant les résultats du compartiment. Vous pouvez revisiter et modifier ces configurations de compartiments à tout moment. Vous pouvez également télécharger vos résultats sous forme de rapport CSV à des fins d'audit.

L'analyseur d'accès IAM pour S3 est disponible gratuitement sur la console Amazon S3. L'analyseur d'accès IAM pour S3 est optimisé par l'analyseur d'accès IAM d' AWS Identity and Access

Management (IAM). Pour utiliser IAM Access Analyzer pour S3 dans la console Amazon S3, vous devez visiter la console IAM et créer un analyseur d'accès externe par région.

Pour plus d'informations sur l'analyseur d'accès IAM, consultez Qu'est-ce que l'analyseur d'accès IAM ? dans le Guide de l'utilisateur IAM. Pour plus d'informations sur l'analyseur d'accès IAM pour S3, consultez les sections suivantes.

Important

- IAM Access Analyzer pour S3 nécessite un analyseur au niveau du compte dans chaque Région AWS cas où vous avez des buckets. Pour utiliser l'analyseur d'accès IAM pour S3, vous devez accéder à l'analyseur d'accès IAM et créer un analyseur doté d'un compte comme zone de confiance. Pour plus d'informations, consultez Activation de l'analyseur d'accès IAM dans le Guide de l'utilisateur IAM.
- L'analyseur d'accès IAM pour S3 n'analyse pas la politique de point d'accès qui est attachée aux points d'accès intercomptes. Ce comportement se produit parce que le point d'accès et sa politique sont en dehors de la zone de confiance, c'est-à-dire du compte. Les compartiments qui délèguent l'accès à un point d'accès intercompte sont répertoriés sous Buckets with public access (Compartiments avec accès public) si vous n'avez pas appliqué le paramètre de blocage de l'accès public `RestrictPublicBuckets` au compartiment ou au compte. Lorsque vous appliquez le paramètre de `RestrictPublicBuckets` blocage de l'accès public, le compartiment est indiqué sous Compartiments accessibles par d'autres Comptes AWS personnes, y compris par des tiers Comptes AWS.
- Lorsqu'une politique de compartiment ou une liste de contrôle d'accès (ACL) de compartiment est ajoutée ou modifiée, l'analyseur d'accès IAM génère et met à jour les résultats en fonction de la modification dans un délai de 30 minutes. Il peut s'écouler jusqu'à six heures avant que les résultats relatifs aux paramètres de blocage de l'accès public au niveau du compte ne soient générés ou mis à jour après la modification des paramètres. Les résultats relatifs aux points d'accès multi-régions ne peuvent pas être générés ou mis à jour pendant six heures au maximum après la création, la suppression d'un point d'accès multi-régions ou la modification de sa politique.

Rubriques

- Révision d'un résumé global des politiques qui accordent un accès externe aux buckets
- Informations fournies par IAM Access Analyzer pour S3

- Blocage de tous les accès publics
- Vérification et modification de l'accès à un compartiment
- Archivage des résultats de compartiment
- Activation d'un résultat de compartiment archivé
- Affichage des détails de résultats
- Téléchargement d'un rapport de l'analyseur d'accès IAM pour S3

Révision d'un résumé global des politiques qui accordent un accès externe aux buckets

Vous pouvez utiliser le résumé des accès externes pour afficher un résumé global des politiques qui accordent un accès externe aux compartiments situés dans votre établissement Compte AWS directement depuis la console S3. Ce résumé vous aide à identifier les compartiments à usage général Amazon S3 dans tous ceux Région AWS qui autorisent l'accès public ou l'accès depuis d'autres utilisateurs Comptes AWS sans avoir à inspecter les politiques de chaque compartiment Région AWS individuellement.

Activation du résumé des accès externes et de l'analyseur d'accès IAM pour S3

Pour utiliser le résumé des accès externes et l'analyseur d'accès IAM pour S3, vous devez suivre les étapes préalables suivantes.

1. Accordez les autorisations requises. Pour plus d'informations, consultez Autorisations requises pour l'utilisation de l'analyseur d'accès IAM dans le Guide de l'utilisateur IAM.
2. Accédez à IAM pour créer un analyseur au niveau du compte pour chaque région où vous souhaitez utiliser l'analyseur d'accès IAM.

   Vous pouvez le faire en créant un analyseur doté d'un compte comme zone de confiance dans la console IAM ou en utilisant le AWS CLI ou. AWS SDKs Pour plus d'informations, consultez Activation de l'analyseur d'accès IAM dans le Guide de l'utilisateur IAM.

Affichage des compartiments autorisant un accès externe

Le résumé de l'accès externe affiche les résultats et les erreurs relatifs à l'accès externe fournis par IAM Access Analyzer pour S3 pour les compartiments à usage général. Les résultats archivés et les résultats relatifs à des accès non utilisés ne sont pas inclus dans le résumé mais peuvent

être consultés dans la console IAM ou IAM Access Analyzer pour S3. Pour plus d'informations, voir Afficher le tableau de bord des résultats d'IAM Access Analyzer dans le guide de l'utilisateur d'IAM.

> **Note**
>
> Le résumé des accès externes inclut uniquement les résultats des analyseurs d'accès externes pour chacun de vous Comptes AWS, et non pour votre AWS organisation.

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, sélectionnez Buckets à usage général.
3. Développez le résumé des accès externes. La console affiche les résultats des accès publics et intercomptes actifs.

   > **Note**
   >
   > Si S3 rencontre un problème lors du chargement des détails du bucket, actualisez la liste des buckets à usage général ou consultez les résultats dans IAM Access Analyzer for S3. Pour de plus amples informations, veuillez consulter Examen de l'accès aux compartiments à l'aide de l'analyseur d'accès IAM pour S3.

4. Pour consulter la liste des résultats ou des erreurs relatifs à un Région AWS, cliquez sur le lien vers la région. La page IAM Access Analyzer pour S3 affiche les noms des compartiments accessibles publiquement ou par d'autres personnes. Comptes AWS Pour de plus amples informations, veuillez consulter Informations fournies par IAM Access Analyzer pour S3.

Mise à jour des contrôles d'accès pour les compartiments autorisant un accès externe

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, sélectionnez Buckets à usage général.
3. Développez le résumé des accès externes. La console affiche les résultats actifs pour les buckets accessibles publiquement ou par d'autres Comptes AWS personnes.

   > **Note**
   >
   > Si S3 rencontre un problème lors du chargement des détails du bucket, actualisez la liste des buckets à usage général ou consultez les résultats dans IAM Access Analyzer

for S3. Pour de plus amples informations, veuillez consulter Examen de l'accès aux compartiments à l'aide de l'analyseur d'accès IAM pour S3.

4. Pour consulter la liste des résultats ou des erreurs relatifs à un Région AWS, cliquez sur le lien vers la région. L'analyseur d'accès IAM pour S3 affiche les résultats actifs pour les buckets accessibles publiquement ou par d'autres personnes. Comptes AWS

> **Note**
>
> Les résultats relatifs aux accès externes figurant dans le résumé des accès externes sont automatiquement mis à jour toutes les 24 heures.

5. Pour bloquer tout accès public à un bucket, consultezBlocage de tous les accès publics. Pour modifier l'accès au bucket, consultezVérification et modification de l'accès à un compartiment.

Informations fournies par IAM Access Analyzer pour S3

L'analyseur d'accès IAM pour S3 fournit des résultats pour les compartiments accessibles hors de votre Compte AWS. Les compartiments répertoriés dans les résultats relatifs à l'accès public sont accessibles à tous sur Internet. Si l'analyseur d'accès IAM pour S3 identifie des compartiments publics, un avertissement en haut de la page indique le nombre de compartiments publics figurant dans votre région. Les compartiments répertoriés dans la section Résultats relatifs à l'accès entre comptes sont partagés de manière conditionnelle avec d'autres utilisateurs Comptes AWS, y compris des comptes extérieurs à votre organisation.

Pour chaque compartiment, l'analyseur d'accès IAM pour S3 fournit les informations suivantes :

- Nom du compartiment
- Shared through (Partagé via) – Mode de partage du compartiment : via une politique de compartiment, une liste de contrôle d'accès (ACL) ou une politique de point d'accès. Les points d'accès multi-régions et les points d'accès intercompte figurent sous la rubrique points d'accès. Un bucket peut être partagé à la fois via des politiques et ACLs. Si vous souhaitez rechercher et examiner la source de votre accès au compartiment, vous pouvez utiliser les informations de cette colonne comme point de départ pour prendre des mesures correctives immédiates et précises.
- Status (Statut) – Statut du résultat de compartiment. L'analyseur d'accès IAM pour S3 affiche les résultats pour tous les compartiments publics et partagés.
  - Active (Actif) – Le résultat n'a pas été vérifié.

  - Archived (Archivé) – Le résultat a été vérifié et confirmé comme prévu.
  - Tous - Tous les résultats relatifs aux compartiments publics ou partagés avec d'autres personnes Comptes AWS, y compris Comptes AWS en dehors de votre organisation.
- Access level (Niveau d'accès) – Autorisations d'accès accordées pour le compartiment :
  - List (Liste) – Répertorier les ressources.
  - Read (Lecture) – Lire mais ne pas modifier les contenus et attributs de ressources.
  - Write (Écriture) – Créer, supprimer ou modifier des ressources.
  - Permissions (Autorisations) – Accorder ou modifier des autorisations de ressources.
  - Tagging (Balisage) – Mettre à jour les balises associées à la ressource.
- Responsable externe - L' Compte AWS extérieur de votre organisation ayant accès au bucket.
- Restriction de la politique de contrôle des ressources (RCP) - La politique de contrôle des ressources (RCP) qui s'applique au compartiment, le cas échéant. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs).

Blocage de tous les accès publics

Si vous souhaitez bloquer tout accès à un compartiment en un seul clic, vous pouvez utiliser le bouton Bloquer tout l'accès public dans l'analyseur d'accès IAM pour S3. Lorsque vous bloquez tout accès public à un compartiment, aucun accès public n'est accordé. Nous vous recommandons de bloquer tous les accès publics à vos compartiments, sauf si vous avez besoin d'un accès public pour prendre en charge un cas d'utilisation spécifique et vérifié. Avant de bloquer tout accès public, assurez-vous que vos applications continueront à fonctionner correctement sans accès public.

Si vous ne souhaitez pas bloquer tous les accès publics à votre compartiment, vous pouvez modifier vos paramètres de blocage de l'accès public dans la console Amazon S3 pour configurer des niveaux d'accès précis à vos compartiments. Pour de plus amples informations, veuillez consulter Blocage de l'accès public à votre stockage Amazon S3.

Dans de rares cas, l'évaluation de l'accès public par bloc IAM Access Analyzer pour S3 et Amazon S3 peut différer selon qu'un bucket est public ou non. Ce comportement est dû au fait qu'Amazon S3 bloque l'accès public et valide l'existence d'actions en plus d'évaluer l'accès public. Supposons que la politique du compartiment contienne une `Action` déclaration qui autorise l'accès public pour une action qui n'est pas prise en charge par Amazon S3 (par exemple,`s3:NotASupportedAction`). Dans ce cas, le blocage de l'accès public par Amazon S3 considère le compartiment comme étant public, car une telle déclaration pourrait potentiellement le rendre public si l'action est prise en charge

ultérieurement. Dans les cas où Amazon S3 bloque l'accès public et IAM Access Analyzer for S3 diffèrent dans leurs évaluations, nous vous recommandons de revoir la politique des compartiments et de supprimer toutes les actions non prises en charge.

Pour bloquer tout accès public à un compartiment à l'aide de l'analyseur d'accès IAM pour S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, sous Dashboards (Tableaux de bord), choisissez Access Analyzer for S3 (Analyseur d'accès pour S3).
3. Dans l'analyseur d'accès IAM pour S3, choisissez un compartiment.
4. Choisissez Block all public access (Bloquer tous les accès publics).
5. Pour confirmer votre intention de bloquer tout accès public au compartiment, dans Block all public access (bucket settings) (Bloquer tout accès public (paramètres du compartiment)), entrez **`confirm`**.

   Amazon S3 bloque tout accès public à votre compartiment. Le statut du résultat de compartiment devient résolu et le compartiment disparaît de la liste de l'analyseur d'accès IAM pour S3. Si vous souhaitez passer en revue les compartiments résolus, ouvrez l'analyseur d'accès IAM dans la console IAM.

Vérification et modification de l'accès à un compartiment

Si vous n'aviez pas l'intention d'accorder l'accès au public ou à d'autres Comptes AWS personnes, y compris à des comptes extérieurs à votre organisation, vous pouvez modifier l'ACL du bucket, la politique du bucket, la politique du point d'accès multirégional ou la politique du point d'accès pour supprimer l'accès au bucket. La colonne Shared through indique toutes les sources d'accès aux compartiments : politique de compartiment, ACL de compartiment, politique de point and/or d'accès. Les points d'accès multi-régions et les points d'accès intercompte figurent sous la rubrique points d'accès.

Pour consulter et modifier une politique de compartiment, une liste ACL de compartiment ou une politique de point d'accès

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Access Analyzer for S3 (Analyseur d'accès pour S3).

3. Pour déterminer si l'accès public ou l'accès partagé est accordé via une politique de compartiment, une liste de contrôle d'accès de compartiment ou une politique de point d'accès, consultez la colonne Shared through (Partagé via).
4. Sous Buckets (Compartiments), choisissez le nom du compartiment avec la politique de compartiment, la liste ACL de compartiment, la politique de point d'accès multi-Régions ou la politique de point d'accès que vous souhaitez modifier ou vérifier.
5. Si vous souhaitez modifier ou consulter la liste ACL d'un compartiment :

   a. Choisissez Permissions.
   b. Choisissez Access Control List.
   c. Consultez la liste ACL de votre compartiment et apportez les modifications nécessaires.

   Pour plus d'informations, consultez Configuration ACLs.
6. Si vous souhaitez modifier ou vérifier une politique de compartiment :

   a. Choisissez Permissions.
   b. Choisissez Stratégie de compartiment.
   c. Vérifiez ou modifiez votre politique de compartiment selon vos besoins.

   Pour plus d'informations, consultez Ajout d'une politique de compartiment à l'aide de la console Amazon S3.
7. Si vous souhaitez consulter ou modifier une politique de point d'accès :

   a. Choisissez Point d'accès multi-Régions.
   b. Choisissez le nom du point d'accès multi-Régions.
   c. Vérifiez ou modifiez votre politique de point d'accès multi-Régions selon vos besoins.

   Pour plus d'informations, consultez Autorisations.
8. Si vous souhaitez consulter ou modifier une politique de point d'accès :

   a. Choisissez des points d'accès pour les compartiments à usage général ou des points d'accès pour les compartiments de répertoire.
   b. Choisissez le nom du point d'accès.
   c. Vérifiez ou modifiez l'accès en fonction de vos besoins.

   Pour plus d'informations, consultez Gestion de vos points d'accès Amazon S3 pour les compartiments à usage général.

Si vous modifiez ou supprimez une liste ACL de compartiment, une politique de compartiment ou une politique de point d'accès pour supprimer l'accès public ou partagé, le statut du compartiment devient « résolu ». Les résultats de compartiment résolus disparaissent de la liste de l'analyseur d'accès IAM pour S3, mais vous pouvez les afficher dans l'analyseur d'accès IAM.

Archivage des résultats de compartiment

Si un bucket accorde l'accès au public ou à d'autres personnes Comptes AWS, y compris à des comptes extérieurs à votre organisation, pour prendre en charge un cas d'utilisation spécifique (par exemple, un site Web statique, des téléchargements publics ou le partage entre comptes), vous pouvez archiver les résultats du bucket. Lorsque vous archivez les résultats d'un compartiment, vous confirmez et enregistrez votre intention de le garder public ou partagé. Les résultats de compartiment archivés restent dans votre liste de l'analyseur d'accès IAM pour S3 pour que vous sachiez toujours quels compartiments sont publics ou partagés.

Pour archiver les résultats de compartiment dans l'analyseur d'accès IAM pour S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez IAM Access Analyzer for S3.
3. Dans l'analyseur d'accès IAM pour S3, choisissez un compartiment actif.
4. Pour confirmer votre intention de rendre ce compartiment accessible au public ou à d'autres personnes Comptes AWS, y compris à des comptes extérieurs à votre organisation, choisissez Archiver.
5. Entrez **`confirm`**, puis choisissez Archive (Archiver).

Activation d'un résultat de compartiment archivé

Après avoir archivé des résultats, vous pouvez toujours les revoir et faire passer leur statut à « actif », ce qui indique que le compartiment nécessite une autre vérification.

Pour activer un résultat de compartiment archivé dans l'analyseur d'accès IAM pour S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Access Analyzer for S3 (Analyseur d'accès pour S3).
3. Choisissez les résultats de compartiment archivés.

4. Choisissez Mark as active (Marquer comme actif).

Affichage des détails de résultats

Si vous souhaitez obtenir plus d'informations sur une découverte, vous pouvez ouvrir les détails de la recherche du compartiment dans IAM Access Analyzer sur la console IAM.

Pour afficher les détails des résultats dans l'analyseur d'accès IAM pour S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Access Analyzer for S3 (Analyseur d'accès pour S3).
3. Dans l'analyseur d'accès IAM pour S3, choisissez un compartiment.
4. Choisissez Afficher les détails.

   Les détails de résultats s'ouvrent dans l'analyseur d'accès IAM de la console IAM.

Téléchargement d'un rapport de l'analyseur d'accès IAM pour S3

Vous pouvez télécharger vos résultats de compartiment sous la forme d'un rapport CSV que vous pouvez utiliser à des fins d'audit. Ce rapport inclut les mêmes informations que celles que vous voyez dans l'analyseur d'accès IAM pour S3 dans la console Amazon S3.

Pour télécharger un rapport

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Access Analyzer for S3 (Analyseur d'accès pour S3).
3. Dans le filtre de Région, sélectionnez la Région.

   L'analyseur d'accès IAM pour S3 est mis à jour pour afficher les compartiments pour la région choisie.
4. Choisissez Download report (Télécharger le rapport).

   Un rapport CSV est généré et enregistré sur votre ordinateur.

Vérification de la propriété du compartiment avec la condition du propriétaire du compartiment

La condition du propriétaire du compartiment Amazon S3 garantit que les compartiments que vous utilisez dans vos opérations S3 correspondent à vos attentes. Comptes AWS

La plupart des opérations S3 lisent ou écrivent dans des compartiments S3 spécifiques. Ces opérations incluent le chargement, la copie et le téléchargement d'objets, la récupération ou la modification de configurations de compartiments et la récupération ou la modification de configurations d'objets. Lorsque vous exécutez ces opérations, vous spécifiez le compartiment que vous souhaitez utiliser en incluant son nom avec la demande. Par exemple, pour récupérer un objet à partir de S3, vous effectuez une demande qui spécifie le nom d'un compartiment et la clé d'objet à extraire depuis ce compartiment.

Étant donné qu'Amazon S3 identifie les compartiments en fonction de leurs noms, une application qui utilise un nom de compartiment incorrect dans une demande peut effectuer par inadvertance des opérations sur un compartiment différent de ce qui était prévu. Pour éviter les interactions de compartiments involontaires dans des situations comme celle-ci, vous pouvez utiliser la condition propriétaire du compartiment. La condition propriétaire du compartiment vous permet de vérifier que le compartiment cible appartient au Compte AWS prévu, ce qui vous offre une garantie supplémentaire que vos opérations S3 ont les effets souhaités.

Rubriques

- Quand utiliser la condition propriétaire du compartiment
- Vérification d'un propriétaire du compartiment
- Exemples
- Limites et restrictions

Quand utiliser la condition propriétaire du compartiment

Nous vous recommandons d'utiliser la condition propriétaire du compartiment chaque fois que vous exécutez une opération S3 prise en charge et que vous connaissez l'ID de compte du propriétaire du compartiment prévu. La condition propriétaire du compartiment est disponible pour toutes les opérations d'objet S3 et la plupart des opérations de compartiment S3. Pour obtenir la liste des opérations S3 ne prenant pas en charge la condition propriétaire du compartiment, consultez Limites et restrictions.

Pour voir les avantages de l'utilisation de la condition du propriétaire du bucket, imaginez le scénario suivant impliquant le AWS client Bea :

1. Bea développe une application qui utilise Amazon S3. Pendant le développement, Bea utilise ses tests uniquement Compte AWS pour créer un bucket nommébea-data-test, et configure son application pour qu'elle y envoie des demandes. bea-data-test
2. Bea déploie son application, mais oublie de reconfigurer l'application pour qu'elle utilise un compartiment dans son Compte AWS de production.
3. En production, l'application de Bea effectue des demandes réussies à bea-data-test. Cela entraîne l'écriture de données de production dans le compartiment du compte de test de Bea.

Bea peut se protéger contre les situations de ce genre en utilisant la condition propriétaire du compartiment. Avec l'état du propriétaire du bucket, Bea peut inclure l' Compte AWS identifiant du propriétaire attendu du bucket dans ses demandes. Amazon S3 vérifie ensuite l'ID de compte du propriétaire du compartiment avant de traiter chaque demande. Si le propriétaire du compartiment réel ne correspond pas au propriétaire du compartiment prévu, la demande échoue.

Si Bea utilise la condition propriétaire du compartiment, le scénario décrit précédemment n'entraînera pas l'écriture par inadvertance de l'application de Bea dans un compartiment du compte de test. Au lieu de cela, les demandes effectuées par l'application lors de l'étape 3 échoueront avec un message d'erreur Access Denied. En utilisant la condition propriétaire du compartiment, Bea élimine le risque d'interaction accidentelle avec des compartiments dans le mauvais Compte AWS.

Vérification d'un propriétaire du compartiment

Pour utiliser la condition propriétaire du compartiment, vous incluez à votre demande un paramètre qui spécifie le propriétaire du compartiment prévu. La plupart des opérations S3 impliquent seulement un compartiment unique et n'exigent que ce paramètre unique pour utiliser la condition propriétaire du compartiment. Pour les opérations Copy0bject, ce premier paramètre spécifie le propriétaire prévu du compartiment de destination et vous incluez un second paramètre pour spécifier le propriétaire prévu du compartiment source.

Lorsque vous effectuez une demande qui inclut un paramètre de condition propriétaire du compartiment, S3 compare l'ID de compte du propriétaire du compartiment et le paramètre spécifié avant de traiter la demande. Si le paramètre correspond à l'ID de compte du propriétaire du compartiment, S3 traite la demande. Si le paramètre ne correspond pas à l'ID de compte du propriétaire du compartiment, la demande échoue avec un message d'erreur Access Denied.

Vous pouvez utiliser la condition du propriétaire du compartiment avec le AWS Command Line Interface (AWS CLI) AWS SDKs, et Amazon S3 REST APIs. Lorsque vous utilisez la condition du propriétaire du compartiment avec le REST AWS CLI et Amazon S3 APIs, utilisez les noms de paramètres suivants.

Méthode d'accès	Paramètre pour les opérations non copiées	Paramètre source de l'opération Copy	Paramètre de destination de l'opération Copy
AWS CLI	`--expected-bucket-owner`	`--expected-source-bucket-owner`	`--expected-bucket-owner`
Amazon S3 REST APIs	En-tête `x-amz-expected-bucket-owner`	En-tête `x-amz-source-expected-bucket-owner`	En-tête `x-amz-expected-bucket-owner`

Les noms de paramètres requis pour utiliser la condition du propriétaire du compartiment AWS SDKs varient en fonction de la langue. Pour déterminer les paramètres requis, consultez la documentation du kit SDK correspondant à la langue souhaitée. Vous trouverez la documentation du kit SDK dans Outils pour créer sur AWS.

Exemples

Les exemples suivants montrent comment implémenter la condition du propriétaire du compartiment dans Amazon S3 à l'aide du AWS CLI ou du AWS SDK for Java 2.x.

Example

Exemple : Chargement d'un objet

L'exemple suivant charge un objet dans le compartiment S3 *amzn-s3-demo-bucket1* à l'aide de la condition propriétaire du compartiment pour s'assurer que *amzn-s3-demo-bucket1* appartient au Compte AWS 111122223333.

AWS CLI

```
aws s3api put-object \
```

```
                --bucket amzn-s3-demo-bucket1 --key exampleobject --
body example_file.txt \
                --expected-bucket-owner 111122223333
```

AWS SDK for Java 2.x

```
public void putObjectExample() {
    S3Client s3Client = S3Client.create();;
    PutObjectRequest request = PutObjectRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
            .key("exampleobject")
            .expectedBucketOwner("111122223333")
            .build();
    Path path = Paths.get("example_file.txt");
    s3Client.putObject(request, path);
}
```

Example

Exemple : Copie d'un objet

L'exemple suivant copie l'objet `object1` à partir du compartiment S3 *amzn-s3-demo-bucket1* vers le compartiment S3 *amzn-s3-demo-bucket2*. Il utilise la condition propriétaire du compartiment pour s'assurer que les compartiments appartiennent aux comptes prévus en fonction du tableau suivant.

Compartiment	Propriétaire prévu
amzn-s3-demo-bucket1	111122223333
amzn-s3-demo-bucket2	444455556666

AWS CLI

```
aws s3api copy-object --copy-source amzn-s3-demo-bucket1/object1 \
                          --bucket amzn-s3-demo-bucket2 --key object1copy \
                          --expected-source-bucket-owner 111122223333 --expected-
bucket-owner 444455556666
```

AWS SDK for Java 2.x

```
public void copyObjectExample() {
        S3Client s3Client = S3Client.create();
        CopyObjectRequest request = CopyObjectRequest.builder()
                .copySource("amzn-s3-demo-bucket1/object1")
                .destinationBucket("amzn-s3-demo-bucket2")
                .destinationKey("object1copy")
                .expectedSourceBucketOwner("111122223333")
                .expectedBucketOwner("444455556666")
                .build();
        s3Client.copyObject(request);
    }
```

Example

Exemple : Récupération d'une politique de compartiment

L'exemple suivant récupère la stratégie d'accès pour le compartiment S3 *amzn-s3-demo-bucket1* à l'aide de la condition propriétaire du compartiment pour s'assurer que *amzn-s3-demo-bucket1* appartient au Compte AWS 111122223333.

AWS CLI

```
aws s3api get-bucket-policy --bucket amzn-s3-demo-bucket1 --expected-bucket-
owner 111122223333
```

AWS SDK for Java 2.x

```
public void getBucketPolicyExample() {
    S3Client s3Client = S3Client.create();
    GetBucketPolicyRequest request = GetBucketPolicyRequest.builder()
            .bucket("amzn-s3-demo-bucket1")
            .expectedBucketOwner("111122223333")
            .build();
    try {
        GetBucketPolicyResponse response = s3Client.getBucketPolicy(request);
    }
    catch (S3Exception e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
```

```
    }
}
```

Limites et restrictions

La condition propriétaire du compartiment Amazon S3 comporte les restrictions et limitations suivantes :

- La valeur du paramètre de condition du propriétaire du compartiment doit être un Compte AWS ID (valeur numérique à 12 chiffres). Les principals de service ne sont pas pris en charge.
- La condition de propriétaire du bucket n'est pas disponible pour CreateBucketou aucune des opérations incluses dans AWS S3 Control. ListBuckets Amazon S3 ignore tous les paramètres de condition propriétaire du compartiment inclus dans les demandes envoyées à ces opérations.
- La condition propriétaire du compartiment vérifie uniquement que le compartiment appartient au compte spécifié dans le paramètre de vérification. La condition propriétaire du compartiment ne vérifie pas la configuration du compartiment. Elle ne garantit pas non plus que la configuration du compartiment remplit des conditions spécifiques ou correspond à un état antérieur.

Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour contrôler la propriété des objets chargés dans votre compartiment et pour désactiver ou activer les listes de contrôle d'accès () ACLs. Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket et tous ACLs sont désactivés. Lorsqu'elles ACLs sont désactivées, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs, et nous vous recommandons de le ACLs désactiver, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler plus facilement l'accès à chaque objet de votre compartiment, quelle que soit la personne qui a chargé les objets dans votre compartiment.

La propriété des objets comporte trois paramètres que vous pouvez utiliser pour contrôler la propriété des objets chargés dans votre bucket et pour désactiver ou activer ACLs :

ACLs handicapé

- Appliqués par le propriétaire du compartiment (par défaut) : ACLs sont désactivés, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. ACLs n'affectent plus les autorisations relatives aux données du compartiment S3. Le compartiment utilise des stratégies pour définir le contrôle des accès.

ACLs enabled

- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.
- Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

Pour la majorité des cas d'utilisation modernes de S3, nous vous recommandons de conserver la ACLs désactivation en appliquant le paramètre d'application obligatoire du propriétaire du compartiment et en utilisant votre politique de compartiment pour partager des données avec des utilisateurs extérieurs à votre compte selon les besoins. Cette approche simplifie la gestion des autorisations. Vous pouvez ACLs le désactiver à la fois sur les buckets nouvellement créés et sur les buckets déjà existants. Pour les buckets nouvellement créés, ACLs ils sont désactivés par défaut. Dans le cas d'un compartiment existant qui contient déjà des objets, une fois que vous l'avez désactivé ACLs, l'objet et le compartiment ne ACLs font plus partie d'une évaluation de l'accès, et l'accès est accordé ou refusé sur la base de politiques. Pour les buckets existants, vous pouvez les réactiver ACLs à tout moment après les avoir désactivés, et votre bucket et votre objet ACLs préexistants seront restaurés.

Avant de procéder à la désactivation ACLs, nous vous recommandons de consulter votre politique relative aux compartiments afin de vous assurer qu'elle couvre toutes les manières dont vous avez l'intention d'accorder l'accès à votre compartiment en dehors de votre compte. Après la désactivation ACLs, votre compartiment accepte uniquement les PUT demandes qui ne spécifient pas d'ACL ou les PUT demandes avec le contrôle total du propriétaire du bucket ACLs, par exemple, l'`bucket-owner-full-control`ACL prédéfinie ou des formes équivalentes de cette ACL exprimées en XML. Les applications existantes qui prennent en charge le contrôle total du propriétaire du ACLs bucket n'ont aucun impact. PUTles demandes qui en contiennent d'autres ACLs (par exemple, des autorisations personnalisées accordées à certains Comptes AWS) échouent et renvoient une `400` erreur avec le code d'erreur`AccessControlListNotSupported`.

En revanche, un bucket avec le paramètre préféré du propriétaire du bucket continue d'accepter et de respecter le bucket et l'objet ACLs. Avec ce paramètre, de nouveaux objets écrits avec la liste ACL `bucket-owner-full-control` prédéfinie sont automatiquement détenus par le propriétaire du compartiment plutôt que par l'auteur d'objets. Tous les autres comportements ACL restent en place. Pour exiger que toutes les opérations PUT Amazon S3 incluent la liste ACL `bucket-owner-full-control` prédéfinie, vous pouvez ajouter une politique de compartiment qui n'autorise que les chargements d'objets à l'aide de cette ACL.

Pour voir quels paramètres de propriété d'objets sont appliqués à vos compartiments, vous pouvez utiliser les métriques Amazon S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Pour plus d'informations, consultez Using S3 Storage Lens to find Object Ownership settings (Utilisation de S3 Storage Lens pour trouver les paramètres de propriété des objets).

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Paramètres de la propriété de l'objet

Ce tableau montre l'impact de chaque paramètre de propriété des objets sur les objets ACLs, la propriété des objets et les téléchargements d'objets.

Paramètre	S'applique à	Effet sur la propriété de l'objet	Effet sur ACLs	Chargements acceptés
Propriétaire du compartiment appliqué (par défaut)	Tous les objets existants et nouveaux	Le propriétaire du compartiment est propriétaire de chaque objet.	ACLs sont désactivés et n'affectent plus les autorisations d'accès à votre compartiment. Les demandes	Téléversements avec le contrôle total du propriétaire du compartiment ACLs ou téléchargements

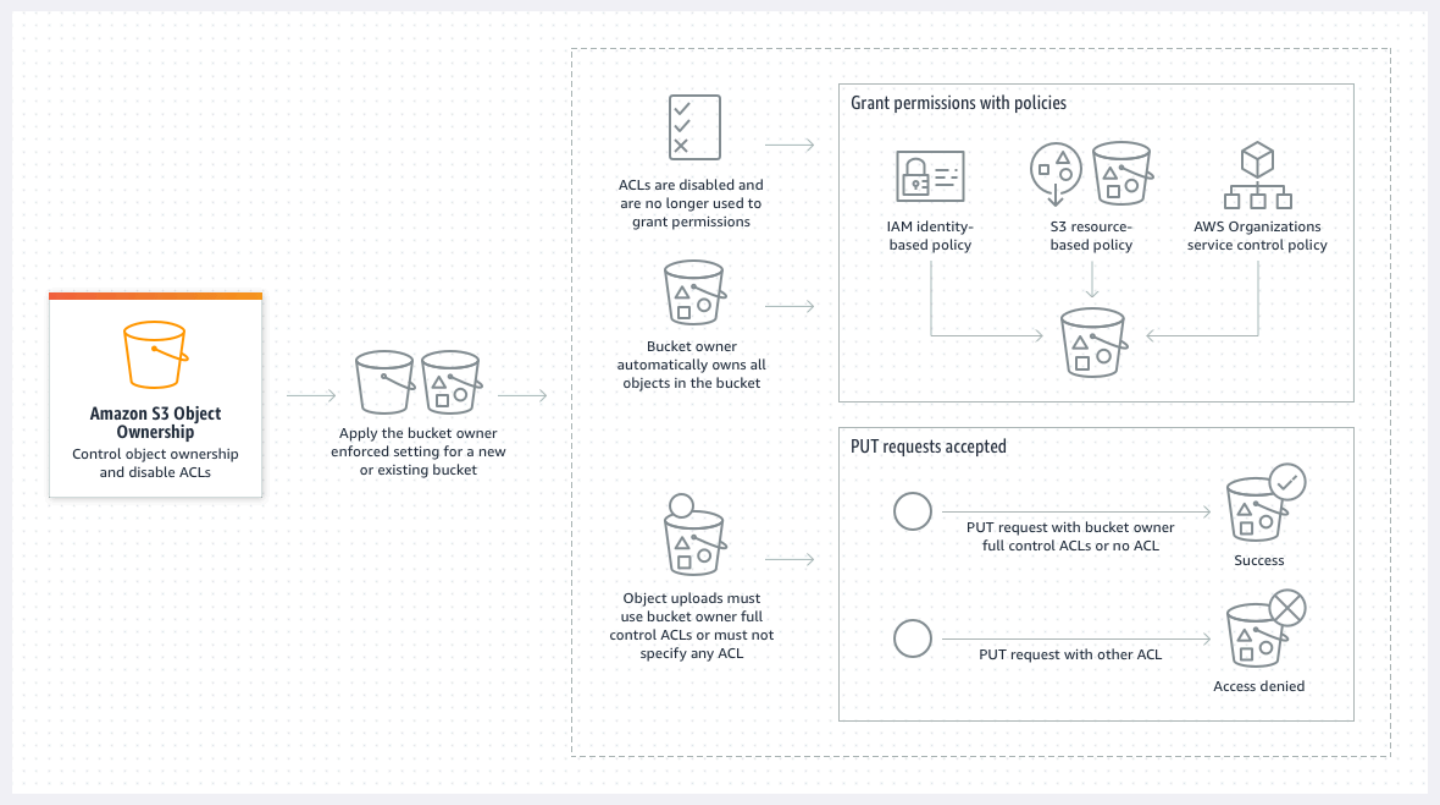
Paramètre	S'applique à	Effet sur la propriété de l'objet	Effet sur ACLs	Chargements acceptés
			de configuration ou de mise à jour ACLs échouent. Cependant, les demandes de lecture ACLs sont prises en charge. Le propriétaire du compartiment possède la propriété et le contrôle complets. Le rédacteur d'objets n'a plus la propriété et le contrôle complets.	ne spécifiant pas d'ACL

Paramètre	S'applique à	Effet sur la propriété de l'objet	Effet sur ACLs	Chargements acceptés
Propriétaire du compartiment préféré	Nouveaux objets	Si le chargement d'un objet inclut la liste ACL `bucket-owner-full-control` prédéfinie, le propriétaire du compartiment est propriétaire de l'objet. Les objets chargés avec d'autres objets ACLs appartiennent au compte d'écriture.	ACLs peut être mis à jour et peut accorder des autorisations. Si le chargement d'un objet inclut la liste ACL `bucket-owner-full-control` prédéfinie, le propriétaire du compartiment dispose d'un accès en contrôle total et l'enregistreur d'objets n'a plus d'accès de contrôle complet.	Tous les chargements
Créateur d'objets	Nouveaux objets	Le rédacteur d'objet possède l'objet.	ACLs peut être mis à jour et peut accorder des autorisations. Le rédacteur d'objet dispose d'un accès complet.	Tous les chargements

Modifications apportées par la désactivation ACLs

Lorsque le paramètre imposé par le propriétaire du compartiment pour la propriété des objets est appliqué, ACLs il est désactivé et vous possédez automatiquement tous les objets du compartiment et vous en prenez le contrôle total sans effectuer d'actions supplémentaires. Propriétaire du compartiment appliqué est le paramètre par défaut pour tous les compartiments nouvellement créés. Après l'application du paramètre Propriétaire du compartiment appliqué, trois changements sont notables :

- Tous les compartiments ACLs et objets ACLs sont désactivés, ce qui vous donne un accès complet en tant que propriétaire du compartiment. Lorsque vous exécutez une demande ACL en lecture sur votre compartiment ou votre objet, vous verrez que l'accès complet n'est accordé qu'au propriétaire du compartiment.
- Avec ce paramètre, en tant que propriétaire du compartiment, vous possédez automatiquement tous les objets de votre compartiment.
- ACLs n'affecte plus les autorisations d'accès à votre bucket. Par conséquent, le contrôle d'accès à vos données est basé sur des politiques, telles que les politiques basées sur l'identité AWS Identity and Access Management (IAM), les politiques relatives aux compartiments Amazon S3, les politiques relatives aux points de terminaison VPC et les politiques de contrôle des services des Organizations (SCPs) ou les politiques de contrôle des ressources (). RCPs



Si vous utilisez la gestion des versions S3, le propriétaire du compartiment possède et contrôle total sur toutes les versions d'objets de votre compartiment. L'application du paramètre Propriétaire du compartiment appliqué n'ajoute pas de nouvelle version d'un objet.

Les nouveaux objets ne peuvent être chargés dans votre bucket que s'ils utilisent le contrôle total du propriétaire du bucket ACLs ou s'ils ne spécifient pas d'ACL. Les téléchargements d'objets échouent s'ils spécifient une autre liste ACL. Pour de plus amples informations, veuillez consulter Résolution des problèmes.

Étant donné que l'exemple d'`PutObject`opération suivant utilisant le AWS Command Line Interface (AWS CLI) inclut l'`bucket-owner-full-control`ACL prédéfinie, l'objet peut être chargé dans un bucket lorsque cette option est désactivée ACLs.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file --
acl bucket-owner-full-control
```

Comme l'`PutObject`opération suivante ne spécifie pas d'ACL, elle réussit également pour un bucket désactivé ACLs.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key key-name --body path-to-file
```

> **Note**
>
> Si d'autres utilisateurs Comptes AWS ont besoin d'accéder aux objets après le téléchargement, vous devez accorder des autorisations supplémentaires à ces comptes par le biais de politiques relatives aux compartiments. Pour de plus amples informations, veuillez consulter Procédures détaillées qui utilisent des politiques pour gérer l'accès à vos ressources Amazon S3.

Réactivation ACLs

Vous pouvez le réactiver ACLs en passant du paramètre imposé au propriétaire du compartiment à un autre paramètre de propriété de l'objet à tout moment. Si vous avez utilisé un objet ACLs pour la gestion des autorisations avant d'appliquer le paramètre imposé au propriétaire du compartiment et que vous n'avez pas migré ces autorisations ACL d'objet vers votre politique de compartiment ACLs, ces autorisations sont restaurées une fois que vous les avez réactivées. De plus, les objets écrits dans le compartiment pendant que le paramètre Propriétaire du compartiment appliqué était appliqué appartiennent toujours au propriétaire du compartiment.

Par exemple, si du paramètre Propriétaire du compartiment appliqué vous revenez au paramètre Créateur d'objets, en tant que propriétaire du compartiment, vous ne possédez plus les objets qui appartenaient auparavant à d'autres Comptes AWS, et n'en avez plus le contrôle total. Au lieu de cela, les comptes de chargement sont à nouveau propriétaires de ces objets. Les objets appartenant à d'autres comptes utilisent ACLs des autorisations. Vous ne pouvez donc pas utiliser de politiques pour accorder des autorisations à ces objets. Toutefois, en tant que propriétaire du compartiment, vous possédez toujours les objets qui ont été écrits dans le compartiment quand le paramètre Propriétaire du compartiment appliqué était appliqué. Ces objets ne sont pas la propriété de l'auteur de l'objet, même si vous les réactivez ACLs.

Pour obtenir des instructions sur l'activation et la gestion à l' ACLs AWS Management Console aide de l'API REST AWS Command Line Interface (CLI) AWS SDKs, ou consultezConfiguration ACLs.

Conditions préalables à la désactivation ACLs

Avant de procéder à ACLs la désactivation pour un bucket existant, remplissez les conditions préalables suivantes.

- Passez en revue le bucket et l'objet ACLs et migrez les autorisations ACL

- Identifier toutes les demandes qui ont nécessité une liste ACL pour l'autorisation
- Vérifiez et mettez à jour les stratégies de compartiment qui utilisent des clés de condition associées à ACL

Autorisations de propriété d'objet

Pour appliquer, mettre à jour ou supprimer un paramètre de propriété d'objet pour un compartiment, vous devez utiliser l'autorisation `s3:PutBucketOwnershipControls`. Pour renvoyer le paramètre propriété de l'objet d'un compartiment, vous devez utiliser l'autorisation `s3:GetBucketOwnershipControls`. Pour plus d'informations, consultez Définition de la propriété d'objet lors de la création d'un compartiment et Affichage du paramètre de propriété d'objet pour un compartiment S3.

Désactivation ACLs pour tous les nouveaux buckets

Par défaut, tous les nouveaux compartiments sont créés avec le paramètre appliqué par le propriétaire du compartiment et ACLs sont désactivés. Nous vous recommandons de rester ACLs handicapé. En règle générale, nous recommandons d'utiliser des politiques basées sur les ressources S3 (politiques de compartiment et politiques de point d'accès) ou des politiques IAM pour le contrôle d'accès au lieu de. ACLs Les politiques constituent une option de contrôle d'accès simplifiée et plus flexible. Les politiques de compartiment et de point d'accès vous permettent de définir des règles s'appliquant de manière générale à toutes les demandes adressées à vos ressources Amazon S3.

Réplication et propriété d'objet

Lorsque vous utilisez la réplication S3 et que les compartiments source et de destination appartiennent à des propriétaires différents Comptes AWS, vous pouvez les désactiver ACLs (en appliquant le paramètre propriétaire du compartiment pour la propriété de l'objet) pour remplacer la propriété de la réplique par Compte AWS celle qui possède le compartiment de destination. Ce paramètre imite le comportement de remplacement du propriétaire existant sans avoir besoin d'une autorisation `s3:ObjectOwnerOverrideToBucketOwner`. Tous les objets répliqués dans le compartiment de destination avec le paramètre Propriétaire du compartiment appliqué appartiennent au propriétaire du compartiment de destination. Pour plus d'informations sur l'option

de remplacement du propriétaire pour les configurations de réplication, consultez Modification du propriétaire d'un réplica.

Définition de la propriété de l'objet

Vous pouvez appliquer un paramètre de propriété d'objet à l'aide de la console Amazon S3, AWS CLI, AWS SDKs, de l'API REST Amazon S3 ou AWS CloudFormation. L'API et les AWS CLI commandes REST suivantes prennent en charge la propriété des objets :

API REST	AWS CLI	Description
PutBucketOwnershipControls	put-bucket-ownership-controls	Crée ou modifie le paramètre de propriété d'objet pour un compartiment S3 existant.
CreateBucket	create-bucket	Crée un compartiment à l'aide de l'en-tête de demande `x-amz-object-ownership` pour spécifier le paramètre de Propriété d'objet.
GetBucketOwnershipControls	get-bucket-ownership-controls	Extrait le paramètre de propriété d'objet pour un compartiment Amazon S3.
DeleteBucketOwnershipControls	delete-bucket-ownership-controls	Supprime le paramètre de propriété d'objet pour un compartiment Amazon S3.

Pour plus d'informations sur l'application et l'utilisation des paramètres de propriété d'objet, consultez les rubriques suivantes.

Rubriques

- Conditions préalables à la désactivation ACLs
- Définition de la propriété d'objet lors de la création d'un compartiment
- Définition de la propriété d'un objet sur un compartiment existant
- Affichage du paramètre de propriété d'objet pour un compartiment S3

- Désactivation ACLs pour tous les nouveaux compartiments et renforcement de la propriété des objets
- Résolution des problèmes

Conditions préalables à la désactivation ACLs

Une liste de contrôle d'accès aux compartiments (ACL) dans Amazon S3 est un mécanisme qui vous permet de définir des autorisations détaillées pour des objets individuels au sein d'un compartiment S3, en spécifiant quels AWS comptes ou groupes peuvent accéder à ces objets et les modifier. La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons d'utiliser des politiques AWS Identity and Access Management (IAM) et de compartiments pour gérer l'accès et pour maintenir la ACLs désactivation, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement.

Si vous l'avez ACLs activé sur votre compartiment, avant de le désactiver ACLs, remplissez les conditions préalables suivantes :

Rubriques

- Passez en revue le bucket et l'objet ACLs et migrez les autorisations ACL
- Identifier toutes les demandes qui ont nécessité une liste ACL pour l'autorisation
- Vérifiez et mettez à jour les stratégies de compartiment qui utilisent des clés de condition associées à ACL
- Exemples de cas d'utilisation

Passez en revue le bucket et l'objet ACLs et migrez les autorisations ACL

Lorsque vous désactivez ACLs, les autorisations accordées par bucket et par objet ACLs n'affectent plus l'accès. Avant de procéder à la désactivation ACLs, passez en revue votre bucket et votre objet ACLs.

Chacun de vos compartiments et objets existants ACLs possède un équivalent dans une politique IAM. Les exemples de politique de compartiment suivants vous montrent comment `READ` `WRITE` les autorisations relatives aux compartiments et aux objets sont ACLs associées aux autorisations IAM. Pour plus d'informations sur la façon dont chaque liste ACL se traduit par des autorisations IAM, consultez Mappage des autorisations de liste ACL et de stratégie d'accès.

Avant de désactiver ACLs :

- Si l'ACL de votre bucket accorde l'accès en dehors de votre AWS compte, vous devez d'abord migrer les autorisations ACL de votre bucket vers votre politique de bucket.
- Ensuite, redéfinissez l'ACL de votre bucket sur l'ACL privée par défaut.
- Nous vous recommandons également de revoir vos autorisations ACL au niveau de l'objet et de les migrer vers votre politique de compartiment.

Si votre compartiment ACLs accorde des autorisations de lecture ou d'écriture à d'autres personnes extérieures à votre compte, avant de pouvoir les désactiver ACLs, vous devez migrer ces autorisations vers votre politique de compartiment. Après avoir migré ces autorisations, vous pouvez attribuer à la propriété de l'objet le paramètre imposé par le propriétaire du compartiment. Si vous ne migrez pas un bucket ACLs qui accorde un accès en lecture ou en écriture en dehors de votre compte, votre demande d'application du paramètre imposé par le propriétaire du bucket échoue et renvoie le code InvalidBucketAclWithObjectOwnershipd'erreur.

Si l'ACL de votre bucket accorde un accès en dehors de votre bucket Compte AWS, avant de désactiver ACLs, vous devez migrer les autorisations ACL de votre bucket vers votre politique de bucket et réinitialiser votre ACL de bucket sur l'ACL privée par défaut. Si vous ne migrez pas et ne réinitialisez pas, votre demande d'application du paramètre de désactivation imposé par le propriétaire du bucket ACLs échoue et renvoie le code InvalidBucketAclWithObjectOwnershipd'erreur. Nous vous recommandons également de revoir les autorisations ACL de votre objet et de les migrer vers votre politique de compartiment.

Pour consulter et migrer les autorisations ACL vers des stratégies de compartiment, consultez les rubriques suivantes.

Rubriques

- Exemples de stratégies de compartiment
- Utilisation de la console S3 pour réviser et migrer les autorisations ACL
- Utilisation du AWS CLI pour vérifier et migrer les autorisations ACL

Exemples de stratégies de compartiment

Ces exemples de politiques de compartiment vous montrent comment migrer les autorisations ACL de `WRITE` compartiment `READ` et d'objet pour un tiers Compte AWS vers une politique de compartiment. `READ_ACP`et `WRITE_ACP` ACLs sont moins pertinents pour les politiques car ils accordent des autorisations liées à l'ACL (`s3:GetBucketAcl`, `s3:GetObjectAcls3:PutBucketAcl`, ets`3:PutObjectAcl`).

Example : liste ACL **READ** pour un compartiment

Si votre bucket dispose d'une READ ACL qui Compte AWS *111122223333* autorise la liste du contenu de votre bucket, vous pouvez écrire une politique de bucket qui accorde `s3:ListBucket` `s3:ListBucketMultipartUploads` des autorisations pour votre bucket. `s3:ListBucketVersions`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to list the objects in a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [

      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:ListBucket",
     "s3:ListBucketVersions",
     "s3:ListBucketMultipartUploads"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
   }
  ]
 }
```

Example — **READ** ACLs pour chaque objet d'un compartiment

Si chaque objet de votre compartiment dispose d'une READ ACL qui autorise l'accès à Compte AWS *111122223333*, vous pouvez rédiger une politique de compartiment qui accorde `s3:GetObject` des `s3:GetObjectVersion` autorisations à ce compte pour chaque objet de votre compartiment.

JSON

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Read permission for every object in a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:GetObject",
     "s3:GetObjectVersion"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
 }
```

Cet exemple d'élément de ressource accorde l'accès à un objet spécifique.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

Example : liste ACL **WRITE** qui accorde les autorisations d'écriture d'objets dans un compartiment

Si votre compartiment possède une `WRITE` ACL qui Compte AWS *111122223333* autorise l'écriture d'objets dans votre compartiment, vous pouvez rédiger une politique de compartiment qui accorde `s3:PutObject` l'autorisation pour votre compartiment.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "Permission to write objects to a bucket",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
```

```
    },
    "Action": [
     "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*"
   }
  ]
}
```

Utilisation de la console S3 pour réviser et migrer les autorisations ACL

Pour passer en revue les autorisations ACL d'un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, sélectionnez le nom de votre compartiment.
3. Sélectionnez l'onglet Autorisations.
4. Sous Access control list (ACL) (Liste de contrôle d'accès [ACL]), vérifiez les autorisations ACL de votre compartiment.

Pour passer en revue les autorisations ACL d'un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le nom du compartiment qui contient votre objet.
3. Dans la liste Objets, choisissez le nom de votre objet.
4. Sélectionnez l'onglet Autorisations.
5. Sous Access control list (ACL) (Liste de contrôle d'accès [ACL]), vérifiez les autorisations ACL de votre objet.

Pour migrer les autorisations ACL et mettre à jour la liste ACL de votre compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, sélectionnez le nom de votre compartiment.
3. Dans l'onglet Autorisations, sous Politique de compartiment, choisissez Modifier.

4. Dans la boîte Policy (Stratégie), ajoutez ou mettez à jour la politique de compartiment.

   Si vous souhaitez consulter des exemples de politiques de compartiment, consultez Exemples de stratégies de compartiment et Exemples de cas d'utilisation .

5. Sélectionnez Enregistrer les modifications.
6. Mettez à jour la liste ACL de votre compartiment pour supprimer les autorisations ACL à d'autres groupes ou Comptes AWS.
7. Appliquez le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets.

Utilisation du AWS CLI pour vérifier et migrer les autorisations ACL

1. Pour renvoyer l'ACL du bucket correspondant à votre bucket, utilisez la get-bucket-acl AWS CLI commande suivante :

   ```
   aws s3api get-bucket-acl --bucket amzn-s3-demo-bucket
   ```

   Par exemple, cette liste ACL de compartiment accorde l'accès en `WRITE` et en `READ` à un compte tiers. Dans cette liste ACL, le compte tiers est identifié par l'ID d'utilisateur canonique. Pour appliquer le paramètre imposé par le propriétaire du bucket et le désactiver ACLs, vous devez migrer ces autorisations pour le compte tiers vers une politique de bucket.

   ```
   {
     "Owner": {
      "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
      "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
     },
     "Grants": [
      {
       "Grantee": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
        "Type": "CanonicalUser"
       },
       "Permission": "FULL_CONTROL"
      },
      {
       "Grantee": {
        "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
   ```

```
    "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
    "Type": "CanonicalUser"
   },
   "Permission": "READ"
  },
  {
   "Grantee": {
    "DisplayName": "THIRD-PARTY-EXAMPLE-ACCOUNT",
    "ID":
"72806de9d1ae8b171cca9e2494a8d1335dfced4ThirdPartyAccountCanonicalUserID",
    "Type": "CanonicalUser"
   },
   "Permission": "WRITE"
  }
 ]
}
```

Pour un autre exemple ACLs, voirExemples de cas d'utilisation .

2. Migrez les autorisations ACL de votre compartiment vers une politique de compartiment :

   Cet exemple de politique de compartiment accorde des autorisations `s3:PutObject` et `s3:ListBucket` pour un compte tiers. Dans la politique du compartiment, le compte tiers est identifié par l' Compte AWS ID (*111122223333*).

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

 policy.json:
 {
  "Version": "2012-10-17",
  "Statement": [
   {
    "Sid": "PolicyForCrossAccountAllowUpload",
    "Effect": "Allow",
    "Principal": {
     "AWS": [
      "arn:aws:iam::111122223333:root"
     ]
    },
    "Action": [
     "s3:PutObject",
```

```
      "s3:ListBucket"
     ],
     "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket",
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    }
   ]
}
```

Si vous souhaitez consulter d'autres exemples de politiques de compartiment, consultez Exemples de stratégies de compartiment et Exemples de cas d'utilisation .

3. Pour renvoyer l'ACL pour un objet spécifique, utilisez la get-object-acl AWS CLI commande.

```
aws s3api get-object-acl --bucket amzn-s3-demo-bucket --key EXAMPLE-OBJECT-KEY
```

4. Si nécessaire, migrez les autorisations ACL d'objet vers votre politique de compartiment.

   Cet exemple d'élément de ressource accorde l'accès à un objet spécifique dans une politique de compartiment.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-OBJECT-KEY"
```

5. Réinitialisez la liste ACL de votre compartiment à la liste ACL par défaut.

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

6. Appliquez le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets.

Identifier toutes les demandes qui ont nécessité une liste ACL pour l'autorisation

Pour identifier les demandes Amazon S3 nécessitant ACLs une autorisation, vous pouvez utiliser la `aclRequired` valeur dans les journaux d'accès au serveur Amazon S3 ou AWS CloudTrail. Si la demande a nécessité une liste ACL pour l'autorisation ou si vous avez des demandes PUT qui spécifient une liste ACL, la chaîne est `Yes`. Si aucune valeur ACLs n'est requise, ou si vous définissez une ACL `bucket-owner-full-control` prédéfinie, ou si les demandes sont autorisées par votre politique de compartiment, la chaîne de `aclRequired` valeur est « - » dans les journaux d'accès au serveur Amazon S3 et est absente dans CloudTrail. Pour plus d'informations sur les valeurs `aclRequired` attendues, consultez Valeurs `aclRequired` pour les demandes Amazon S3 courantes.

Si vous avez `PutBucketAcl` ou demandez des `PutObjectAcl` en-têtes qui accordent des autorisations basées sur l'ACL, à l'exception de l'ACL `bucket-owner-full-control` prédéfinie, vous devez supprimer ces en-têtes avant de pouvoir les désactiver. ACLs Dans le cas contraire, vos demandes échoueront.

Pour toutes les autres demandes nécessitant une liste ACL pour l'autorisation, migrez ces autorisations de liste ACL vers des politiques de compartiment. Supprimez ensuite tout compartiment ACLs avant d'activer le paramètre imposé par le propriétaire du compartiment.

> **Note**
>
> Ne retirez pas l'objet ACLs. Dans le cas contraire, les applications qui dépendent de l'objet ACLs pour obtenir des autorisations perdront leur accès.

Si vous constatez qu'aucune demande ne nécessitait une ACL pour obtenir une autorisation, vous pouvez procéder à la désactivation ACLs. Pour plus d'informations sur l'identification des demandes, consultez Utilisation des journaux d'accès au serveur Amazon S3 pour identifier des demandes et Identification des demandes Amazon S3 à l'aide de CloudTrail.

Vérifiez et mettez à jour les stratégies de compartiment qui utilisent des clés de condition associées à ACL

Une fois que vous avez appliqué le paramètre de désactivation obligatoire du propriétaire du compartiment ACLs, les nouveaux objets ne peuvent être chargés dans votre compartiment que si la demande utilise le contrôle total du propriétaire du compartiment ACLs ou ne spécifie pas d'ACL. Avant de procéder à la désactivation ACLs, consultez votre politique de compartiment en ce qui concerne les clés de condition liées à l'ACL.

Si votre politique de compartiment utilise une clé de condition associée à la liste ACL pour exiger la liste ACL `bucket-owner-full-control` prédéfinie (par exemple, `s3:x-amz-acl`), vous n'avez pas besoin de mettre à jour votre politique de compartiment. La politique de compartiment suivante utilise la `s3:x-amz-acl` pour exiger la liste ACL `bucket-owner-full-control` prédéfinie pour les demandes `PutObject` S3. Cette politique demande encore au rédacteur d'objets qu'il spécifie la liste ACL `bucket-owner-full-control` prédéfinie. Cependant, les buckets ACLs désactivés acceptent toujours cette ACL, de sorte que les demandes continuent de réussir sans qu'aucune modification côté client ne soit requise.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with bucket owner full
 control",
            "Effect": "Allow",
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"
                ]
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::example-s3-bucket;/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Cependant, si votre politique de compartiment utilise une clé de condition associée à la liste ACL qui nécessite une liste ACL différente, vous devez supprimer cette clé de condition. Cet exemple de politique de compartiment nécessite l'`public-read`ACL pour les `PutObject` requêtes S3 et doit donc être mis à jour avant la désactivation ACLs.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Only allow writes to my bucket with public read access",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": [
                    "arn:aws:iam::111122223333:user/ExampleUser"                ]
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "StringEquals": {
                    "s3:x-amz-acl": "public-read"
                }
            }
        }
    ]
}
```

Exemples de cas d'utilisation

Les exemples suivants vous montrent comment migrer les autorisations ACL vers des stratégies de compartiment pour des cas d'utilisation spécifiques.

Rubriques

- Octroi de l'accès au groupe de livraison des journaux S3 pour la journalisation des accès au serveur
- Accordez un accès public en lecture aux objets se trouvant dans un compartiment.
- Accordez à Amazon ElastiCache (Redis OSS) l'accès à votre compartiment S3

Octroi de l'accès au groupe de livraison des journaux S3 pour la journalisation des accès au serveur

Si vous souhaitez appliquer le paramètre activé par le propriétaire du compartiment à désactiver ACLs pour un compartiment de destination de journalisation de l'accès au serveur (également appelé compartiment cible), vous devez faire migrer les autorisations ACL du bucket pour le groupe de mise à disposition de journaux S3 vers le principal du service de journalisation (`logging.s3.amazonaws.com`) dans une politique de compartiment. Pour plus d'informations sur les autorisations de la diffusion des journaux, consultez Autorisations de diffusion de journaux.

Ce compartiment ACL accorde un accès en `WRITE` et en `READ_ACP` au groupe de mise à disposition des journaux S3 :

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "Type": "CanonicalUser",
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/s3/LogDelivery"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

Pour migrer les autorisations ACL du compartiment pour le groupe de mise à disposition du journal S3 vers le principal du service de journalisation dans une politique de compartiment

1. Ajoutez la politique de compartiment suivante à votre compartiment de destination, en remplaçant les exemples de valeurs.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy file://
policy.json

policy.json:      {
```

```
    {
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/EXAMPLE-LOGGING-PREFIX*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::SOURCE-BUCKET-NAME"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-AWS-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

2. Réinitialisez la liste ACL de votre compartiment de destination sur la liste ACL par défaut.

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. Appliquez le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets à votre compartiment de destination.

Accordez un accès public en lecture aux objets se trouvant dans un compartiment.

Si votre objet ACLs accorde un accès public en lecture à tous les objets de votre compartiment, vous pouvez migrer ces autorisations ACL vers une politique de compartiment.

Cette liste ACL d'objet accorde un accès public en lecture à un objet dans un compartiment :

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
```

```
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

Pour migrer les autorisations ACL publiques en lecture vers une politique de compartiment

1. Pour accorder un accès public en lecture à tous les objets de votre compartiment, ajoutez la politique de compartiment suivante, en remplaçant les exemples de valeurs.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
```

```
        }
    ]
}
```

Pour accorder l'accès public à un objet spécifique dans une politique de compartiment, utilisez le format suivant pour l'élément `Resource`.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/OBJECT-KEY"
```

Pour accorder l'accès public à tous les objets avec un préfixe spécifique, utilisez le format suivant pour l'élément `Resource`.

```
"Resource": "arn:aws:s3:::amzn-s3-demo-bucket/PREFIX/*"
```

2. Appliquez le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets

Accordez à Amazon ElastiCache (Redis OSS) l'accès à votre compartiment S3

Vous pouvez exporter votre sauvegarde ElastiCache (Redis OSS) vers un compartiment S3, ce qui vous permet d'accéder à la sauvegarde depuis l'extérieur ElastiCache. Pour exporter votre sauvegarde vers un compartiment S3, vous devez autoriser ElastiCache la copie d'un instantané dans le compartiment. Si vous avez accordé des autorisations ElastiCache à une ACL de compartiment, vous devez migrer ces autorisations vers une politique de compartiment avant d'appliquer le paramètre de désactivation imposé par le propriétaire du compartiment ACLs. Pour plus d'informations, consultez la section Accorder l' ElastiCache accès à votre compartiment Amazon S3 dans le guide de ElastiCache l'utilisateur Amazon.

L'exemple suivant montre les autorisations ACL du bucket qui accordent des autorisations à ElastiCache.

```
{
    "Owner": {
        "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "DisplayName": "DOC-EXAMPLE-ACCOUNT-OWNER",
```

```
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "WRITE"
        },
        {
            "Grantee": {
                "DisplayName": "aws-scs-s3-readonly",
                "ID":
 "540804c33a284a299d2547575ce1010f2312ef3da9b3a053c8bc45bf233e4353",
                "Type": "CanonicalUser"
            },
            "Permission": "READ_ACP"
        }
    ]
}
```

Pour migrer les autorisations ACL du bucket pour ElastiCache (Redis OSS) vers une politique de bucket

1. Ajoutez la politique de compartiment suivante à votre compartiment, en remplaçant les exemples de valeurs.

```
aws s3api put-bucket-policy --bucket amzn-s3-demo-bucket --policy
 file://policy.json

policy.json:
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Stmt15399483",
            "Effect": "Allow",
            "Principal": {
                "Service": "Region.elasticache-snapshot.amazonaws.com"
            },
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketAcl",
                "s3:ListMultipartUploadParts",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket",
                "arn:aws:s3:::amzn-s3-demo-bucket/*"
            ]
        }
    ]
}
```

2. Réinitialisez la liste ACL de votre compartiment à la liste ACL par défaut :

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-bucket --acl private
```

3. Appliquez le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets

Définition de la propriété d'objet lors de la création d'un compartiment

Lorsque vous créez un compartiment, vous pouvez configurer la propriété d'objet S3. Pour définir la propriété d'un objet pour un compartiment existant, voir Définition de la propriété d'un objet sur un compartiment existant.

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour désactiver les listes de contrôle d'accès (ACLs) et prendre possession de chaque objet de votre compartiment, simplifiant ainsi la gestion des accès aux données stockées dans Amazon S3. Par défaut, S3 Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket et ACLs est désactivé pour les nouveaux buckets. Lorsque cette option est ACLs désactivée, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement.

La propriété des objets comporte trois paramètres que vous pouvez utiliser pour contrôler la propriété des objets chargés dans votre bucket et pour désactiver ou activer ACLs :

ACLs handicapé

- Appliqués par le propriétaire du compartiment (par défaut) : ACLs sont désactivés, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. ACLs n'affectent plus les autorisations relatives aux données du compartiment S3. Le compartiment utilise des stratégies pour définir le contrôle des accès.

ACLs enabled

- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.
- Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

Permissions (Autorisations) : pour appliquer le paramètre Bucket owner enforced (Propriétaire du compartiment imposé) ou le paramètre Bucket owner preferred (Propriétaire du compartiment préféré), vous devez disposer des autorisations suivantes : `s3:CreateBucket` et `s3:PutBucketOwnershipControls`. Aucune autorisation supplémentaire n'est nécessaire lors de la création d'un compartiment avec le paramètre Object writer (Rédacteur d'objets) appliqué. Pour plus d'informations sur les autorisations Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

> **Important**
>
> La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs, et nous vous recommandons de le désactiver, ACLs sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Avec Object Ownership, vous pouvez désactiver les politiques de contrôle d'accès ACLs et vous appuyer sur celles-ci. Lorsque vous le désactivez ACLs, vous pouvez facilement gérer un bucket contenant des objets téléchargés par différents AWS comptes. En tant que propriétaire du compartiment, vous êtes propriétaire de tous les objets du compartiment et pouvez gérer l'accès à ces derniers au moyen de stratégies.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.

   > **Note**
   >
   > - Une fois le compartiment créé, vous ne pouvez pas changer sa région.
   > - Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste d'Amazon S3 Régions AWS, consultez la section sur les Service AWS points de terminaison dans le Référence générale d'Amazon Web Services.

3. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
4. Choisissez Créer un compartiment. La page Créer un compartiment s'ouvre.
5. Pour Nom du compartiment, saisissez le nom de votre compartiment.

   Le nom du compartiment doit présenter les caractéristiques suivantes :

   - Être unique dans une partition. Une partition est un regroupement de régions. AWS possède actuellement trois partitions : `aws` (Régions commerciales), `aws-cn` (Régions de Chine) et `aws-us-gov` (AWS GovCloud (US) Regions).

- Il doit comporter entre 3 et 63 caractères.
- Composé uniquement de lettres minuscules, de chiffres, de points (.) et de traits d'union (). - Pour une compatibilité optimale, nous vous recommandons d'éviter d'utiliser des points (.) dans les noms de bucket, sauf pour les buckets utilisés uniquement pour l'hébergement de sites Web statiques.
- Il doit commencer et se terminer par une lettre ou un chiffre.
- Pour obtenir la liste complète des règles de dénomination des compartiments, consultez. Règles de dénomination des compartiments à usage général

> **Important**
>
> - Une fois le compartiment créé, vous ne pouvez pas changer son nom.
> - N'incluez pas d'informations sensibles dans le nom du bucket. Le nom du bucket est visible URLs là où pointent les objets du bucket.

6. (Facultatif) Sous Configuration générale, vous pouvez choisir de copier les paramètres d'un bucket existant dans votre nouveau bucket. Si vous ne souhaitez pas copier les paramètres d'un bucket existant, passez à l'étape suivante.

> **Note**
>
> Cette option :
>
> - N'est pas disponible dans la console Amazon S3 AWS CLI et n'est disponible que dans la console Amazon S3
> - Ne copie pas la politique du compartiment existant vers le nouveau compartiment

Pour copier les paramètres d'un compartiment existant, sous Copier les paramètres d'un compartiment existant, sélectionnez Choisir un compartiment. La fenêtre Choisir un compartiment s'ouvre. Recherchez le compartiment contenant les paramètres que vous souhaitez copier, puis sélectionnez Choisir un compartiment. La fenêtre Choisir un compartiment se ferme et la fenêtre Créer un compartiment s'ouvre à nouveau.

Sous Copier les paramètres d'un bucket existant, vous pouvez désormais voir le nom du bucket que vous avez sélectionné. Les paramètres de votre nouveau compartiment correspondent

désormais aux paramètres du compartiment que vous avez sélectionné. Si vous souhaitez supprimer les paramètres copiés, choisissez Restaurer les paramètres par défaut. Passez en revue les autres paramètres du bucket sur la page Créer un bucket. Si vous ne souhaitez apporter aucune modification, vous pouvez passer à l'étape finale.

7. Sous Propriété des objets, pour désactiver ou activer ACLs et contrôler la propriété des objets chargés dans votre bucket, sélectionnez l'un des paramètres suivants :

   ACLs handicapé

   - Application par le propriétaire du compartiment (par défaut) : ACLs cette option est désactivée, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment à usage général et en a le contrôle total. ACLs n'affectent plus les autorisations d'accès aux données du compartiment à usage général S3. Le compartiment utilise des stratégies exclusivement pour définir le contrôle des accès.

     Par défaut, ACLs sont désactivés. La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

   ACLs enabled

   - Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.

     Si vous appliquez le paramètre Propriétaire du compartiment préféré, pour exiger que tous les chargements Amazon S3 incluent la liste ACL prédéfinie `bucket-owner-full-control`, vous pouvez ajouter une politique de compartiment qui autorise uniquement les chargements d'objets utilisant cette liste ACL.

   - Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

> **Note**
>
> Le paramètre par défaut est Propriétaire du compartiment appliqué. Pour appliquer le paramètre par défaut et le maintenir ACLs désactivé, seule l'`s3:CreateBucket`autorisation est nécessaire. Pour l'activer ACLs, vous devez avoir l'`s3:PutBucketOwnershipControls`autorisation.

8. Dans Paramètres de blocage de l'accès public pour ce compartiment, choisissez les paramètres Bloquer l'accès public que vous souhaitez appliquer au compartiment.

   Par défaut, les quatre paramètres de blocage de l'accès public sont activés. Nous vous recommandons de maintenir tous les paramètres activés, sauf si vous savez que vous devez en désactiver un ou plusieurs pour votre cas d'utilisation spécifique. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.

   > **Note**
   >
   > Pour activer tous les paramètres de blocage de l'accès public, seule l'autorisation `s3:CreateBucket` est requise. Pour désactiver les paramètres de blocage de l'accès public, vous devez disposer de l'autorisation `s3:PutBucketPublicAccessBlock`.

9. (Facultatif) Par défaut, le versionnement des compartiments est désactivé. La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans un même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment. Le contrôle de version permet de récupérer facilement les données en cas d'action involontaire d'un utilisateur ou de défaillance applicative. Pour plus d'informations sur la gestion des versions, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

   Pour activer le versionnement sur votre compartiment, choisissez Enable.

10. (Facultatif) Sous Tags (Balises), vous pouvez choisir d'ajouter des balises à votre compartiment. Avec la répartition des AWS coûts, vous pouvez utiliser des balises de compartiment pour annoter la facturation liée à l'utilisation d'un compartiment. Une balise correspond à une paire clé-valeur représentant un libellé que vous affectez à un compartiment. Pour de plus amples informations, veuillez consulter the section called "Utilisation des balises de répartition des coûts".

Pour ajouter une balise de compartiment, saisissez une Key (Clé) et éventuellement une Value (Valeur), puis choisissez Add Tag (Ajouter une balise).

11. Pour configurer le chiffrement par défaut, sous Type de chiffrement, sélectionnez l'une des options suivantes :

    - Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
    - Chiffrement côté serveur avec AWS Key Management Service clés (SSE-KMS)
    - Chiffrement double couche côté serveur avec clés AWS Key Management Service (AWS KMS) (DSSE-KMS)

    > **Important**
    >
    > Si vous utilisez l'option SSE-KMS ou DSSE-KMS pour votre configuration de chiffrement par défaut, vous êtes soumis au quota de demandes par seconde (RPS) de. AWS KMS Pour plus d'informations sur les AWS KMS quotas et sur la manière de demander une augmentation de quota, consultez la section Quotas dans le guide du AWS Key Management Service développeur.

    Les buckets et les nouveaux objets sont chiffrés en utilisant le chiffrement côté serveur avec les clés gérées Amazon S3 (SSE-S3) comme niveau de base de configuration de chiffrement. Pour plus d'informations sur le chiffrement par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Pour en savoir plus sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

    Pour plus d'informations sur l'utilisation du chiffrement côté serveur pour chiffrer vos données, consultez. the section called “Chiffrement des données”

12. Si vous avez choisi le chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3) ou le chiffrement côté serveur double couche avec des clés () AWS Key Management Service (DSSE-KMS AWS KMS), procédez comme suit :

    a. Sous CléAWS KMS , spécifiez votre clé KMS de l'une des manières suivantes :

        - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans la liste des clés disponibles.

La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

- Pour saisir l'ARN de la clé KMS, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de votre clé KMS dans le champ qui s'affiche.
- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

  Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS appartenant à un autre compte, vous devez d'abord être autorisé à utiliser la clé, puis saisir l'ARN de la clé KMS. Pour plus d'informations sur les autorisations entre comptes pour les clés KMS, consultez la section Création de clés KMS utilisables par d'autres comptes dans le guide du AWS Key Management Service développeur. Pour en savoir plus sur SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS). Pour en savoir plus sur DSSE-KMS, consultez the section called "Chiffrement double couche côté serveur (DSSE-KMS)".
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez Identification des clés KMS symétriques et asymétriques dans le Guide du développeur AWS Key Management Service .

b. Lorsque vous configurez votre compartiment pour utiliser le chiffrement par défaut avec SSE-KMS, vous pouvez également utiliser les clés de compartiment S3. Les clés de compartiment S3 réduisent le coût du chiffrement en diminuant le trafic de demandes

d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3. Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS.

Par défaut, les clés de compartiment S3 sont activées dans la console Amazon S3. Nous vous recommandons de laisser les clés de compartiment S3 activées pour réduire vos coûts. Pour désactiver les clés de compartiment S3 pour votre compartiment, sous Clé de compartiment, choisissez Disable.

13. (Facultatif) S3 Object Lock permet de protéger les nouveaux objets contre la suppression ou le remplacement. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet. Si vous souhaitez activer S3 Object Lock, procédez comme suit :

    a. Choisissez Paramètres avancés.

    > **Important**
    >
    > L'activation d'Object Lock active automatiquement le versionnement du bucket. Après avoir activé et créé le bucket avec succès, vous devez également configurer les paramètres de rétention par défaut et de conservation légale d'Object Lock dans l'onglet Propriétés du bucket.

    b. Pour activer le verrouillage d'objets, choisissez Enable (Activer), lisez l'avertissement qui s'affiche et confirmez-le.

    > **Note**
    >
    > Pour créer un bucket activé pour Object Lock, vous devez disposer des autorisations suivantes : `s3:CreateBuckets3:PutBucketVersioning`, `ets3:PutBucketObjectLockConfiguration`.

14. Choisissez Créer un compartiment.

À l'aide du AWS CLI

Pour définir la propriété de l'objet lorsque vous créez un nouveau compartiment, utilisez la `create-bucket` AWS CLI commande avec le `--object-ownership` paramètre.

Cet exemple applique le paramètre Propriétaire du compartiment appliqué à un nouveau compartiment à l'aide de l'interface AWS CLI :

```
aws s3api create-bucket --bucket  amzn-s3-demo-bucket --region us-east-1 --object-
ownership BucketOwnerEnforced
```

> **Important**
>
> Si vous ne définissez pas la propriété de l'objet lorsque vous créez un bucket à l'aide de AWS CLI, le paramètre par défaut sera `ObjectWriter` (ACLs activé).

Utilisation du AWS SDK pour Java

Cet exemple définit le paramètre Propriétaire du compartiment appliqué à un nouveau compartiment à l'aide du kit AWS SDK pour Java :

```
    // Build the ObjectOwnership for CreateBucket
    CreateBucketRequest createBucketRequest = CreateBucketRequest.builder()
            .bucket(bucketName)
            .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
            .build()

     // Send the request to Amazon S3
     s3client.createBucket(createBucketRequest);
```

En utilisant AWS CloudFormation

Pour utiliser la `AWS::S3::Bucket` AWS CloudFormation ressource afin de définir la propriété de l'objet lorsque vous créez un nouveau bucket, reportez-vous OwnershipControlsAWS::S3::Bucketau Guide de l'AWS CloudFormation utilisateur.

Utilisation de l'API REST

Pour appliquer le paramètre Propriétaire du compartiment appliqué pour la propriété d'objets S3, utilisez l'opération d'API `CreateBucket` avec l'en-tête de demande `x-amz-object-ownership` défini sur `BucketOwnerEnforced`. Pour plus d'informations et des exemples, consultez CreateBucket dans la Référence d'API Amazon Simple Storage Service.

Étapes suivantes : une fois que vous avez appliqué les paramètres Propriétaire du compartiment appliqué ou Propriétaire du compartiment préféré pour Propriété d'objets, vous pouvez suivre les étapes suivantes :

- Obligation imposée par le propriétaire du bucket — Exigez que tous les nouveaux compartiments soient créés et ACLs désactivés en utilisant une politique IAM ou Organizations.
- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Ajoutez une politique de compartiment S3 pour exiger que la liste ACL `bucket-owner-full-control` prédéfinie pour tous les téléchargements d'objets vers votre compartiment.

Définition de la propriété d'un objet sur un compartiment existant

Vous pouvez configurer la propriété des objets S3 sur un compartiment S3 existant. Pour appliquer la propriété d'objet lors de la création d'un compartiment, consultez Définition de la propriété d'objet lors de la création d'un compartiment.

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour désactiver les listes de contrôle d'accès (ACLs) et prendre possession de chaque objet de votre compartiment, simplifiant ainsi la gestion des accès aux données stockées dans Amazon S3. Par défaut, S3 Object Ownership est défini sur le paramètre imposé par le propriétaire du compartiment et ACLs est désactivé pour les nouveaux compartiments. Lorsque cette option est ACLs désactivée, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement.

La propriété des objets comporte trois paramètres que vous pouvez utiliser pour contrôler la propriété des objets chargés dans votre bucket et pour désactiver ou activer ACLs :

ACLs handicapé

- Appliqués par le propriétaire du compartiment (par défaut) : ACLs sont désactivés, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. ACLs n'affectent plus les autorisations relatives aux données du compartiment S3. Le compartiment utilise des stratégies pour définir le contrôle des accès.

ACLs enabled

- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.
- Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

Conditions préalables : avant d'appliquer le paramètre de désactivation obligatoire par le propriétaire du bucket ACLs, vous devez migrer les autorisations ACL du bucket vers les politiques du bucket et réinitialiser votre bucket ACLs avec l'ACL privée par défaut. Nous vous recommandons également de migrer les autorisations ACL des objets vers les politiques de compartiment et de modifier les politiques de compartiment qui nécessitent un contrôle total ACLs autre que le propriétaire du compartiment ACLs. Pour de plus amples informations, veuillez consulter Conditions préalables à la désactivation ACLs.

Autorisations : pour pouvoir utiliser cette opération, vous devez disposer de l'autorisation `s3:PutBucketOwnershipControls`. Pour plus d'informations sur les autorisations Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le nom du compartiment auquel vous souhaitez appliquer le paramètre de propriété d'objet S3.
3. Choisissez l'onglet Permissions (Autorisations).
4. Sous Object Ownership (Propriétaire de l'objet), sélectionnez Edit (Modifier).
5. Sous Propriété des objets, pour désactiver ou activer ACLs et contrôler la propriété des objets chargés dans votre bucket, sélectionnez l'un des paramètres suivants :

ACLs handicapé

- Appliqués par le propriétaire du compartiment : ACLs ils sont désactivés, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. ACLs n'affectent plus les autorisations relatives aux données du compartiment S3. Le compartiment utilise des stratégies pour définir le contrôle des accès.

  Pour exiger que tous les nouveaux compartiments soient créés et ACLs désactivés à l'aide d'IAM ou de AWS Organizations politiques, consultez. Désactivation ACLs pour tous les nouveaux compartiments (obligatoire par le propriétaire du compartiment)

ACLs enabled

- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.

  Si vous appliquez le paramètre préféré par le propriétaire du compartiment pour exiger que tous les téléchargements Amazon S3 incluent la liste ACL `bucket-owner-full-control`prête à l'emploi, vous pouvez ajouter une politique de compartiment qui autorise uniquement les téléchargements d'objets utilisant cette liste ACL.
- Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

6. Choisissez Enregistrer.

À l'aide du AWS CLI

Pour appliquer un paramètre de propriété d'objet à un compartiment existant, utilisez la commande `put-bucket-ownership-controls`avec le paramètre `--ownership-controls`. Les valeurs valides pour la propriété sont `BucketOwnerEnforced`, `BucketOwnerPreferred` ou `ObjectWriter`.

Cet exemple applique le paramètre Propriétaire du compartiment appliqué pour un compartiment existant à l'aide de l' AWS CLI :

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-
controls="Rules=[{ObjectOwnership=BucketOwnerEnforced}]"
```

Pour plus d'informations sur `put-bucket-ownership-controls`, consultez la rubrique put-bucket-ownership-controls dans le Guide de l'utilisateur AWS Command Line Interface .

Utilisation du AWS SDK pour Java

Cet exemple applique le paramètre `BucketOwnerEnforced` de Propriété d'objet à un compartiment existant à l'aide d' AWS SDK pour Java :

```
        // Build the ObjectOwnership for BucketOwnerEnforced
        OwnershipControlsRule rule = OwnershipControlsRule.builder()
               .objectOwnership(ObjectOwnership.BucketOwnerEnforced)
               .build();

        OwnershipControls ownershipControls = OwnershipControls.builder()
                  .rules(rule)
                  .build()

         // Build the PutBucketOwnershipControlsRequest
         PutBucketOwnershipControlsRequest putBucketOwnershipControlsRequest =
               PutBucketOwnershipControlsRequest.builder()
                       .bucket(BUCKET_NAME)
                       .ownershipControls(ownershipControls)
                       .build();

         // Send the request to Amazon S3
         s3client.putBucketOwnershipControls(putBucketOwnershipControlsRequest);
```

En utilisant AWS CloudFormation

À utiliser AWS CloudFormation pour appliquer un paramètre de propriété d'objet à un bucket existant, consultez AWS::S3::Bucket OwnershipControlsle guide de AWS CloudFormation l'utilisateur.

Utilisation de l'API REST

Pour utiliser l'API REST afin d'appliquer un paramètre de propriété d'objet à un compartiment S3 existant, utilisez `PutBucketOwnershipControls`. Pour plus d'informations, consultez PutBucketOwnershipControls dans la Référence d'API Amazon Simple Storage Service.

Étapes suivantes : une fois que vous avez appliqué les paramètres Propriétaire du compartiment appliqué ou Propriétaire du compartiment préféré pour Propriété d'objets, vous pouvez suivre les étapes suivantes :

- Obligation imposée par le propriétaire du bucket — Exigez que tous les nouveaux compartiments soient créés et ACLs désactivés en utilisant une politique IAM ou Organizations.
- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Ajoutez une stratégie de compartiment S3 pour exiger que la liste ACL `bucket-owner-full-control` prédéfinie pour tous les téléchargements d'objets vers votre compartiment.

Affichage du paramètre de propriété d'objet pour un compartiment S3

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour désactiver les listes de contrôle d'accès (ACLs) et prendre possession de chaque objet de votre compartiment, simplifiant ainsi la gestion des accès aux données stockées dans Amazon S3. Par défaut, S3 Object Ownership est défini sur le paramètre imposé par le propriétaire du compartiment et ACLs est désactivé pour les nouveaux compartiments. Lorsque cette option est ACLs désactivée, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement.

La propriété des objets comporte trois paramètres que vous pouvez utiliser pour contrôler la propriété des objets chargés dans votre bucket et pour désactiver ou activer ACLs :

ACLs handicapé

- Appliqués par le propriétaire du compartiment (par défaut) : ACLs sont désactivés, et le propriétaire du compartiment possède automatiquement tous les objets du compartiment et en a le contrôle total. ACLs n'affectent plus les autorisations relatives aux données du compartiment S3. Le compartiment utilise des stratégies pour définir le contrôle des accès.

ACLs enabled

- Bucket owner preferred (Préféré par le propriétaire du compartiment) – Le propriétaire du compartiment possède les nouveaux objets que d'autres comptes écrivent dans le compartiment avec la liste ACL `bucket-owner-full-control` prête à l'emploi, et en a le contrôle total.

- Auteur d'objets : celui Compte AWS qui télécharge un objet est propriétaire de l'objet, en a le contrôle total et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de celui-ci.

Vous pouvez afficher les paramètres de propriété d'objet S3 pour un compartiment Amazon S3. Pour définir la propriété d'un objet pour un nouveau compartiment, voir Définition de la propriété d'objet lors de la création d'un compartiment. Pour définir la propriété d'un objet pour un compartiment existant, voir Définition de la propriété d'un objet sur un compartiment existant.

Autorisations : pour pouvoir utiliser cette opération, vous devez disposer de l'autorisation `s3:GetBucketOwnershipControls`. Pour plus d'informations sur les autorisations Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le nom du compartiment auquel vous souhaitez appliquer le paramètre de propriété d'objet.
3. Sélectionnez l'onglet Autorisations.
4. Sous Object Ownership (Propriétaire de l'objet), vous pouvez voir les paramètres de propriété des objets pour votre compartiment.

À l'aide du AWS CLI

Pour récupérer le paramètre de propriété de l'objet S3 pour un compartiment S3, utilisez la get-bucket-ownership-controls AWS CLI commande.

```
aws s3api get-bucket-ownership-controls --bucket amzn-s3-demo-bucket
```

Utilisation de l'API REST

Pour récupérer le paramètre Propriété de l'objet pour un compartiment S3, utilisez l'opération `GetBucketOwnershipControls` d'API. Pour de plus amples informations, veuillez consulter GetBucketOwnershipControls.

Désactivation ACLs pour tous les nouveaux compartiments et renforcement de la propriété des objets

Nous vous recommandons de ACLs le désactiver sur vos compartiments Amazon S3. Vous pouvez le faire en appliquant le paramètre Propriétaire du compartiment appliqué pour la propriété d'objets S3. Lorsque vous appliquez ce paramètre, ils ACLs sont désactivés et vous êtes automatiquement propriétaire de tous les objets de votre bucket et vous en avez le contrôle total. Pour exiger que tous les nouveaux compartiments soient créés avec cette option ACLs désactivée, utilisez les politiques AWS Identity and Access Management (IAM) ou les politiques de contrôle des AWS Organizations services (SCPs), comme décrit dans la section suivante.

Pour imposer la propriété des nouveaux objets sans les désactiver ACLs, vous pouvez appliquer le paramètre préféré du propriétaire du compartiment. Lorsque vous appliquez ce paramètre, nous vous recommandons vivement de mettre à jour votre politique de compartiment afin d'exiger la liste ACL `bucket-owner-full-control` prédéfinie pour toutes les demandes PUT envoyées à votre compartiment. Les clients doivent également être mis à jour pour envoyer la liste ACL `bucket-owner-full-control` prédéfinie dans votre compartiment à partir d'autres comptes.

Rubriques

- Désactivation ACLs pour tous les nouveaux compartiments (obligatoire par le propriétaire du compartiment)
- Exiger l' bucket-owner-full-controlACL prédéfini pour les PUT opérations Amazon S3 (préféré du propriétaire du compartiment)

Désactivation ACLs pour tous les nouveaux compartiments (obligatoire par le propriétaire du compartiment)

L'exemple suivant de politique IAM refuse l'autorisation `s3:CreateBucket` pour un rôle ou un utilisateur IAM spécifique, sauf si le paramètre Propriétaire du compartiment appliqué est appliqué pour Propriété d'objets. La paire de clé-valeur dans le bloc `Condition` spécifie `s3:x-amz-object-ownership` comme sa clé et le paramètre `BucketOwnerEnforced` comme sa valeur. En d'autres termes, l'utilisateur IAM ne peut créer des compartiments que s'il définit le paramètre obligatoire pour le propriétaire du compartiment pour la propriété des objets et s'il le désactive. ACLs Vous pouvez également utiliser cette politique comme SCP limite pour votre AWS organisation.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "RequireBucketOwnerFullControl",
            "Action": "s3:CreateBucket",
            "Effect": "Deny",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "s3:x-amz-object-ownership": "BucketOwnerEnforced"
                }
            }
        }
    ]
}
```

Exiger l' bucket-owner-full-controlACL prédéfini pour les **PUT** opérations Amazon S3 (préféré du propriétaire du compartiment)

Avec le paramètre préféré du propriétaire du compartiment pour la propriété de l'objet, vous, en tant que propriétaire du compartiment, possédez et avez le contrôle total sur les nouveaux objets que d'autres comptes écrivent dans votre compartiment avec la liste ACL `bucket-owner-full-control` prédéfinie. Toutefois, si d'autres comptes écrivent des objets dans votre compartiment sans la liste ACL `bucket-owner-full-control` prédéfinie, le rédacteur d'objets conserve son accès total. En tant que propriétaire du compartiment, vous pouvez implémenter une politique de compartiment qui n'autorise les écritures que si elles spécifient la liste ACL `bucket-owner-full-control` prédéfinie.

> **Note**
>
> Si vous l'avez ACLs désactivé avec le paramètre obligatoire pour le propriétaire du compartiment, en tant que propriétaire du compartiment, vous êtes automatiquement propriétaire de tous les objets de votre compartiment et en avez le contrôle total. Vous n'avez pas besoin d'utiliser cette section pour mettre à jour votre politique de compartiment afin d'imposer la propriété de l'objet au propriétaire du compartiment.

La politique de compartiment suivante spécifie que le compte *111122223333* ne peut charger des objets *amzn-s3-demo-bucket* que si la liste ACL de l'objet est définie sur `bucket-owner-full-control`. Veillez à remplacer *111122223333* par voter compte et *amzn-s3-demo-bucket* par le nom de votre compartiment.

JSON

```
{
   "Version": "2012-10-17",
   "Statement": [
      {
         "Sid": "Only allow writes to my bucket with bucket owner full control",
         "Effect": "Allow",
         "Principal": {
            "AWS": [
               "arn:aws:iam::111122223333:user/ExampleUser"
            ]
         },
         "Action": [
            "s3:PutObject"
         ],
         "Resource": "arn:aws:s3:::example-s3-bucket;/*",
         "Condition": {
            "StringEquals": {
               "s3:x-amz-acl": "bucket-owner-full-control"
            }
         }
      }
   ]
}
```

Voici un exemple d'opération de copie qui inclut la liste ACL `bucket-owner-full-control` prédéfinie à l'aide d' AWS Command Line Interface (AWS CLI).

```
aws s3 cp file.txt s3://amzn-s3-demo-bucket --acl bucket-owner-full-control
```

Une fois la politique de compartiment mise en vigueur, si le client n'inclut pas la liste ACL prédéfinie `bucket-owner-full-control`, l'opération échoue et le chargeur reçoit l'erreur suivante :

Une erreur s'est produite (AccessDenied) lors de l'appel de l' PutObject opération : Accès refusé.

> **Note**
>
> Si les clients doivent accéder aux objets après le chargement, vous devez accorder des autorisations supplémentaires au compte de chargement. Pour en savoir plus sur l'octroi aux comptes de l'accès à vos ressources, consultez Procédures détaillées qui utilisent des politiques pour gérer l'accès à vos ressources Amazon S3.

Résolution des problèmes

Lorsque vous appliquez le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, les listes de contrôle d'accès (ACLs) sont désactivées et vous, en tant que propriétaire du compartiment, êtes automatiquement propriétaire de tous les objets de votre compartiment. ACLs n'affecte plus les autorisations pour les objets de votre compartiment. Vous pouvez utiliser des politiques pour accorder des autorisations. Toutes les demandes S3 PUT doivent spécifier la liste ACL prédéfinie `bucket-owner-full-control` ou ne pas spécifier de liste ACL, sinon ces demandes échouent. Pour plus d'informations, consultez Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Si une liste ACL non valide est spécifiée ou si les autorisations ACL de compartiment accordent un accès hors de votre Compte AWS, les erreurs suivantes peuvent s'afficher.

AccessControlListNotSupported

Une fois que vous avez appliqué le paramètre obligatoire du propriétaire du compartiment pour la propriété des objets, ACLs ils sont désactivés. Les demandes de définition ACLs ou de mise à jour ACLs échouent avec une `400` erreur et renvoient le code AccessControlListNotSupportedd'erreur. Les demandes de lecture ACLs sont toujours prises en charge. Les demandes de lecture renvoient ACLs toujours une réponse qui montre que le propriétaire du compartiment a le contrôle total. Dans le cadre de vos PUT opérations, vous devez soit spécifier le contrôle total du propriétaire du bucket, ACLs soit ne pas spécifier d'ACL. Dans le cas contraire, vos opérations PUT échouent.

L'exemple de `put-object` AWS CLI commande suivant inclut l'`public-read`ACL prédéfinie.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object-key-name --body doc-example-body --acl public-read
```

Si le compartiment utilise le paramètre imposé par le propriétaire du compartiment pour le désactiver ACLs, cette opération échoue et le téléchargeur reçoit le message d'erreur suivant :

Une erreur s'est produite (AccessControlListNotSupported) lors de l'appel de l'PutObject opération : le compartiment ne permet pas ACLs

InvalidBucketAclWithObjectOwnership

Si vous souhaitez appliquer le paramètre de désactivation obligatoire au propriétaire du compartiment ACLs, votre ACL de compartiment doit donner le contrôle total uniquement au propriétaire du compartiment. L'ACL de votre bucket ne peut pas donner accès à un groupe externe Compte AWS ou à un autre groupe. Par exemple, si votre `CreateBucket` demande impose le nom du propriétaire du bucket et spécifie une ACL du bucket qui donne accès à une Compte AWS adresse externe, votre demande échoue avec une `400` erreur et renvoie le code InvalidBucketAclWithObjectOwnershipd'erreur. De même, si votre demande `PutBucketOwnershipControls` définit le paramètre appliqué par le propriétaire du compartiment sur un compartiment doté d'une liste ACL de compartiment qui accorde des autorisations à d'autres utilisateurs, la demande échoue.

Example : Une liste ACL de compartiment existante accorde un accès public en lecture.

Par exemple, si une liste ACL de compartiment existante accorde un accès public en lecture, vous ne pouvez pas appliquer le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets tant que vous n'avez pas migré ces autorisations ACL vers une politique de compartiment et que vous n'avez pas réinitialisé votre liste ACL de compartiment à la liste ACL privée par défaut. Pour plus d'informations, consultez Conditions préalables à la désactivation ACLs.

Cet exemple de liste ACL de compartiment existante accorde un accès public en lecture.

```
{
    "Owner": {
        "ID": "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID"
    },
    "Grants": [
        {
            "Grantee": {
                "ID":
 "852b113e7a2f25102679df27bb0ae12b3f85be6BucketOwnerCanonicalUserID",
                "Type": "CanonicalUser"
            },
            "Permission": "FULL_CONTROL"
        },
        {
```

```
            "Grantee": {
                "Type": "Group",
                "URI": "http://acs.amazonaws.com/groups/global/AllUsers"
            },
            "Permission": "READ"
        }
    ]
}
```

L'exemple de `put-bucket-ownership-controls` AWS CLI commande suivant applique le paramètre imposé par le propriétaire du bucket pour Object Ownership :

```
aws s3api put-bucket-ownership-controls --bucket amzn-s3-demo-bucket --ownership-
controls Rules=[{ObjectOwnership=BucketOwnerEnforced}]
```

Étant donné que la liste ACL du compartiment accorde un accès public en lecture, la demande échoue et renvoie le code d'erreur suivant :

Une erreur s'est produite (InvalidBucketAclWithObjectOwnership) lors de l'appel de l' PutBucketOwnershipControls opération : le bucket ne peut pas avoir ACLs défini ObjectOwnership le BucketOwnerEnforced paramètre

Sécurité dans Amazon S3

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 chargé de protéger l'infrastructure qui gère AWS les services dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. L'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de conformitéAWS. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Simple Storage Service (Amazon S3), consultez Services AWS concernés par le 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 organisation ainsi que les lois et réglementations applicables. Pour Amazon S3, votre responsabilité inclut les domaines suivants :

- Gestion de vos données, y compris propriété de l'objet et chiffrement.
- Classification de vos ressources.
- Gestion des accès à vos données à l'aide de rôles IAM et d'autres configurations de service pour appliquer les autorisations appropriées.
- Activation de contrôles de détection tels que AWS CloudTrailAmazon GuardDuty pour Amazon S3.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lorsque vous utilisez Simple Storage Service (Amazon S3). Les rubriques suivantes vous montrent comment configurer Amazon S3 pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui peuvent vous aider à surveiller et à sécuriser vos ressources Amazon S3.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Rubriques

- Bonnes pratiques de sécurité pour Amazon S3
- Protection des données dans Amazon S3
- Protection des données à l'aide du chiffrement
- Confidentialité du trafic inter-réseau
- Validation de conformité pour Amazon S3
- Résilience dans Amazon S3
- Sécurité de l'infrastructure dans Amazon S3
- Configuration et analyse des vulnérabilités dans Amazon S3
- Gestion des accès

Bonnes pratiques de sécurité pour Amazon S3

Amazon S3 fournit différentes fonctions de sécurité à prendre en compte lorsque vous développez et implémentez vos propres stratégies de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des recommandations utiles plutôt que comme des prescriptions.

Rubriques

- Bonnes pratiques en matière de sécurité Amazon S3
- Bonnes pratiques de surveillance et d'audit pour Amazon S3
- Surveillance de la sécurité des données à l'aide AWS de services de sécurité gérés

Bonnes pratiques en matière de sécurité Amazon S3

Les bonnes pratiques suivantes pour Amazon S3 peuvent vous aider à éviter des incidents de sécurité.

Désactiver les listes de contrôle d'accès (ACLs)

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket et tous ACLs sont désactivés. Lorsqu'elles ACLs sont désactivées, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès aux données exclusivement à l'aide de politiques de gestion des accès.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de listes de contrôle d'accès (ACLs). Nous vous recommandons de le désactiver ACLs, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Pour désactiver ACLs et prendre possession de chaque objet de votre compartiment, appliquez le paramètre imposé par le propriétaire du compartiment pour S3 Object Ownership. Lorsque vous le désactivez ACLs, vous pouvez facilement gérer un compartiment contenant des objets chargés par différents utilisateurs Comptes AWS.

Lorsque ACLs le contrôle d'accès à vos données est désactivé, il est basé sur des politiques telles que les suivantes :

- AWS Identity and Access Management politiques utilisateur (IAM)
- Politiques de compartiment S3
- Politiques de point de terminaison de cloud privé virtuel (VPC)
- AWS Organizations politiques de contrôle des services (SCPs)
- AWS Organizations politiques de contrôle des ressources (RCPs)

La désactivation ACLs simplifie la gestion et l'audit des autorisations. ACLs sont désactivés par défaut pour les nouveaux compartiments. Vous pouvez également le désactiver ACLs pour les buckets existants. Si un compartiment existant contient déjà des objets, une fois que vous l'avez désactivé ACLs, l'objet et le compartiment ne ACLs font plus partie du processus d'évaluation des accès. Au lieu de cela, l'accès est accordé ou refusé sur la base des politiques.

Avant de procéder à ACLs la désactivation, assurez-vous d'effectuer les opérations suivantes :

- Passez en revue votre politique de compartiment pour vous assurer qu'elle couvre toutes les façons dont vous avez l'intention d'accorder l'accès à votre compartiment hors de votre compte.
- Réinitialisez votre liste ACL de compartiment à sa valeur par défaut (contrôle total accordé au propriétaire du compartiment).

Après la désactivation ACLs, les comportements suivants se produisent :

- Votre compartiment accepte uniquement les PUT demandes qui ne spécifient pas d'ACL ou les PUT demandes avec le contrôle total du propriétaire du compartiment ACLs. ACLs Il s'agit notamment `bucket-owner-full-control` de l'ACL prédéfinie ou des formes équivalentes de cette ACL exprimées en XML.
- Les applications existantes qui prennent en charge le contrôle total du propriétaire du ACLs bucket n'ont aucun impact.
- PUTles demandes qui en contiennent d'autres ACLs (par exemple, des autorisations personnalisées accordées à certains Comptes AWS) échouent et renvoient un code d'état HTTP `400 (Bad Request)` avec le code d'erreur`AccessControlListNotSupported`.

Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Veillez à ce que vos compartiments Amazon S3 utilisent les stratégies appropriées et ne soient pas accessibles publiquement

À moins que vous ayez explicitement besoin que quiconque sur Internet puisse lire ou écrire dans votre compartiment S3, veillez à ce que votre compartiment S3 ne soit pas public. Voici quelques-unes des étapes que vous pouvez suivre pour bloquer l'accès public :

- Utilisez le blocage de l'accès public S3. Le blocage de l'accès public S3 vous permet de configurer facilement des contrôles centralisés pour limiter l'accès public à vos ressources Amazon S3. Ces contrôles centralisés sont appliqués quelle que soit la manière dont les ressources sont créées. Pour plus d'informations, consultez Blocage de l'accès public à votre stockage Amazon S3.
- Identifiez les politiques de compartiment Amazon S3 qui autorisent une identité à caractère générique telle que `"Principal": "*"` (qui signifie en fait « n'importe qui »). Recherchez également les politiques qui autorisent une action à caractère générique `"*"` (qui permet à l'utilisateur d'effectuer n'importe quelle action dans le compartiment Amazon S3).
- De même, recherchez les listes de contrôle d'accès aux compartiments Amazon S3 (ACLs) qui fournissent un accès en lecture, en écriture ou complet à « tout le monde » ou à « tout AWS utilisateur authentifié ».
- Utilisez l'opération d'API `ListBuckets` pour analyser tous vos compartiments Amazon S3. Utilisez ensuite `GetBucketAcl`, `GetBucketWebsite` et `GetBucketPolicy` pour déterminer si chaque compartiment dispose de contrôles d'accès et d'une configuration conformes.
- Utilisez AWS Trusted Advisor pour inspecter votre implémentation Amazon S3.
- Envisagez de mettre en œuvre des contrôles de détection continus en utilisant les AWS Config Rules gérés s3-bucket-public-read-prohibited et s3-bucket-public-write-prohibited.

Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon S3.

Implémentation d'un accès sur la base du moindre privilège

Lorsque vous accordez des autorisations, vous décidez qui obtient quelles autorisations pour telles ou telles ressources Amazon S3. Vous activez des actions spécifiques que vous souhaitez autoriser sur ces ressources. Par conséquent, nous vous recommandons d'accorder uniquement les autorisations qui sont requises pour effectuer une tâche. L'implémentation d'un accès sur la base du moindre privilège est fondamentale pour réduire les risques en matière de sécurité et l'impact que pourraient avoir des d'erreurs ou des actes de malveillance.

Les outils suivants sont disponibles pour l'implémentation d'un accès sur la base du moindre privilège :

- Actions de politique pour Amazon S3 et Limites d'autorisations pour les entités IAM
- Fonctionnement d'Amazon S3 avec IAM
- Présentation de la liste de contrôle d'accès (ACL)

Pour obtenir des conseils sur ce qu'il faut prendre en compte lors du choix d'un ou plusieurs des mécanismes précédents, consultez Gestion des identités et des accès pour Amazon S3.

Utiliser des rôles IAM pour les applications Services AWS qui nécessitent un accès Amazon S3

Pour que les applications exécutées sur Amazon EC2 ou autre puissent accéder Services AWS aux ressources Amazon S3, elles doivent inclure des AWS informations d'identification valides dans leurs demandes d' AWS API. Nous vous recommandons de ne pas stocker AWS les informations d'identification directement dans l'application ou l' EC2 instance Amazon. Il s'agit d'autorisations à long terme qui ne font pas automatiquement l'objet d'une rotation et qui pourraient avoir un impact commercial important si elles étaient compromises.

À la place, utilisez un rôle IAM pour gérer des autorisations temporaires pour les applications ou services devant accéder à Amazon S3. Lorsque vous utilisez un rôle, vous n'avez pas besoin de distribuer des informations d'identification à long terme (telles qu'un nom d'utilisateur et un mot de passe ou des clés d'accès) à une EC2 instance Amazon ou Service AWS, par exemple AWS Lambda. Le rôle fournit des autorisations temporaires que les applications peuvent utiliser lorsqu'elles appellent d'autres AWS ressources.

Pour plus d'informations, consultez les rubriques suivantes dans le Guide de l'utilisateur IAM :

- Rôles IAM
- Scénarios courants pour les rôles : utilisateurs, applications et services.

Prise en compte du chiffrement de données au repos

Pour protéger des données au repos dans Amazon S3, les options suivantes sont possibles :

- Chiffrement côté serveur : le chiffrement est configuré par défaut pour tous les compartiments Amazon S3, et tous les nouveaux objets qui sont chargés dans un compartiment S3 sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment dans Amazon S3. Pour utiliser un autre type de chiffrement, vous pouvez soit spécifier le type

de chiffrement côté serveur à utiliser dans vos demandes PUT S3, soit définir la configuration de chiffrement par défaut dans le compartiment de destination.

Amazon S3 fournit également les options de chiffrement côté serveur suivantes :

- Chiffrement côté serveur avec clés AWS Key Management Service (AWS KMS) (SSE-KMS)
- Chiffrement double couche côté serveur avec clés AWS Key Management Service (AWS KMS) (DSSE-KMS)
- Chiffrement côté serveur avec clés fournies par le client (SSE-C)

Pour plus d'informations, consultez Protection des données avec le chiffrement côté serveur.

- Chiffrement côté client : chiffrez les données côté client et chargez les données chiffrées dans Amazon S3. Dans ce cas, vous gérez le processus de chiffrement, les clés de chiffrement et les outils associés. Comme le chiffrement côté serveur, le chiffrement côté client peut contribuer à réduire les risques en chiffrant les données avec une clé qui est stockée dans un autre mécanisme que le mécanisme qui stocke les données elles-mêmes.

  Amazon S3 fournit plusieurs options de chiffrement côté client. Pour plus d'informations, consultez Protection des données avec le chiffrement côté client.

Application du chiffrement des données en transit

Vous pouvez utiliser le protocole HTTPS (TLS) pour empêcher les attaquants potentiels d'espionner ou de manipuler le trafic réseau en utilisant des attaques similaires. person-in-the-middle Nous vous recommandons d'autoriser uniquement les connexions chiffrées sur HTTPS (TLS) en utilisant la condition aws:SecureTransport dans vos politiques de compartiment Amazon S3. Pour plus d'informations, consultez l'exemple de politique de compartiment S3 gérant l'accès en fonction de requêtes HTTP ou HTTPS. Outre le refus des requêtes HTTP, nous vous recommandons de configurer des CloudWatch alarmes Amazon pour vous avertir en cas de tentative d'accès HTTP à votre contenu. `tlsDetails.tlsVersion NOT EXISTS` Pour plus d'informations sur la configuration des CloudWatch alarmes Amazon, consultez la section Création d' CloudWatch alarmes pour les CloudTrail événements : exemples et contenu des CloudTrail enregistrements dans le guide de AWS CloudTrail l'utilisateur.

> **Important**
>
> Nous recommandons à votre application de ne pas épingler les certificats TLS Amazon S3 car AWS cela ne prend pas en charge l'épinglage de certificats approuvés par le public. S3 renouvelle automatiquement les certificats, et le renouvellement peut avoir lieu à tout

moment avant leur expiration. Le renouvellement d'un certificat génère une nouvelle paire de clés publique/privée. Si vous avez épinglé un certificat S3 récemment renouvelé avec une nouvelle clé publique, vous ne pourrez pas vous connecter à S3 tant que votre application n'aura pas utilisé le nouveau certificat.

Envisagez également de mettre en œuvre des contrôles de détection continus en utilisant la règle AWS Config gérée s3-bucket-ssl-requests-only.

Prise en compte de l'utilisation du verrouillage des objets S3

Avec le verrouillage des objets S3, vous pouvez stocker des objets en utilisant un modèle « Write Once Read Many » (WORM). Le verrouillage des objets S3 peut contribuer à empêcher une suppression accidentelle ou inappropriée de données. Par exemple, vous pouvez utiliser S3 Object Lock pour protéger vos AWS CloudTrail journaux.

Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

Activation de la gestion des versions S3

La gestion des versions S3 est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment. La gestion des versions permet de récupérer facilement les données en cas d'actions involontaires des utilisateurs ou de défaillances des applications.

Envisagez également de mettre en œuvre des contrôles de détection continus en utilisant la règle AWS Config gérée s3-bucket-versioning-enabled.

Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Prise en compte de l'utilisation de la réplication entre régions Amazon S3

Même si Amazon S3 stocke par défaut vos données dans plusieurs zones de disponibilité distinctes géographiquement, les exigences de conformité peuvent vous obliger à stocker les données à des distances encore plus importantes. Avec S3 Cross-Region Replication (CRR), vous pouvez répliquer des données entre des sites distants Régions AWS pour répondre à ces exigences. Le CRR permet de copier automatiquement et de manière asynchrone des objets dans différents compartiments. Régions AWS Pour de plus amples informations, veuillez consulter Réplication d'objets au sein des régions et entre elles.

> **Note**
>
> La réplication CRR exige que la gestion des versions soit activée pour les compartiments S3 source et de destination.

Envisagez également de mettre en œuvre des contrôles de détection continus en utilisant la règle AWS Config gérée s3-bucket-replication-enabled.

Prise en compte de l'utilisation des points de terminaison de VPC pour l'accès Amazon S3

Un point de terminaison de VPC (Virtual Private Cloud) pour Amazon S3 est une entité logique au sein d'un VPC qui autorise la connectivité uniquement à Amazon S3. Les points de terminaison VPC peuvent empêcher le trafic de traverser le réseau Internet ouvert.

Les points de terminaison VPC pour Amazon S3 offrent plusieurs façons de contrôler l'accès à vos données Amazon S3 :

- Vous pouvez contrôler les demandes, les utilisateurs ou les groupes autorisés à traverser un point de terminaison de VPC spécifique en utilisant des politiques de compartiment S3.
- Vous pouvez contrôler quels points de terminaison VPCs ou quels points de terminaison VPC ont accès à vos compartiments S3 en utilisant les politiques relatives aux compartiments S3.
- Vous pouvez éviter l'exfiltration de données en utilisant un VPC qui ne comporte pas de passerelle Internet.

Pour de plus amples informations, veuillez consulter Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment.

Utilisez des services AWS de sécurité gérés pour surveiller la sécurité des données

Plusieurs services AWS de sécurité gérés peuvent vous aider à identifier, évaluer et surveiller les risques de sécurité et de conformité pour vos données Amazon S3. Ces services peuvent également vous aider à protéger vos données contre ces risques. Ces services incluent des fonctionnalités de détection, de surveillance et de protection automatisées conçues pour passer des ressources Amazon S3 réservées à une seule personne Compte AWS à des ressources destinées aux organisations comptant des milliers de comptes.

Pour de plus amples informations, veuillez consulter Surveillance de la sécurité des données à l'aide AWS de services de sécurité gérés.

Bonnes pratiques de surveillance et d'audit pour Amazon S3

Les bonnes pratiques suivantes pour Amazon S3 peuvent vous aider à détecter les vulnérabilités et les incidents de sécurité potentiels.

Identification et audit de tous vos compartiments Amazon S3

L'identification de vos ressources informatiques est un aspect crucial de la gouvernance et de la sécurité. Vous devez avoir une visibilité sur toutes vos ressources Amazon S3 pour évaluer leur niveau de sécurité et agir sur les zones de vulnérabilité potentielles. Pour auditer vos ressources, nous vous recommandons de procéder comme suit :

- Utilisez Tag Editor pour identifier et baliser les ressources sensibles en matière de sécurité ou d'audit, puis utilisez ces identifications pour rechercher ces ressources. Pour plus d'informations, consultez la section Recherche de ressources à étiqueter dans le Guide de l'utilisateur AWS des ressources de balisage.
- Utilisez l'inventaire S3 pour auditer et signaler le statut de réplication et de chiffrement de vos objets à des fins professionnelles, de conformité et d'obligations réglementaires. Pour plus d'informations, consultez Catalogage et analyse de vos données avec l'inventaire S3.
- Créez des groupes de ressources pour vos ressources Amazon S3. Pour plus d'informations, consultez Que sont les groupes de ressources ? dans le Guide de l'utilisateur AWS Resource Groups .

Mettre en œuvre la surveillance à l'aide d'outils AWS de surveillance

La surveillance joue un rôle important dans le maintien de la fiabilité, de la sécurité, de la disponibilité et des performances d'Amazon S3 et de vos AWS solutions. AWS fournit plusieurs outils et services pour vous aider à surveiller Amazon S3 et vos autres Services AWS. Par exemple, vous pouvez surveiller CloudWatch les métriques Amazon pour Amazon S3, en particulier les `DeleteRequests` métriques `PutRequests` `GetRequests4xxErrors`,, et. Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch et Journalisation et surveillance dans Amazon S3.

Pour obtenir un deuxième exemple, consultez Exemple : Activité de compartiment Amazon S3. Cet exemple décrit comment créer une CloudWatch alarme qui est déclenchée lorsqu'un appel d'API Amazon S3 est envoyé à une politique de compartiment, à `PUT` `DELETE` un cycle de vie de compartiment, à une configuration de réplication de compartiment ou à `PUT` une ACL de compartiment.

Activation de la journalisation des accès au serveur Amazon S3

La journalisation des accès au serveur fournit des enregistrements détaillés sur les demandes soumises à un compartiment. Les journaux d'accès au serveur peuvent vous aider pour les audits de sécurité et d'accès, et vous permettre d'en savoir plus sur votre base de clients et de comprendre votre facture Amazon S3. Pour obtenir des instructions pour l'activation de la journalisation des accès au serveur, consultez Enregistrement de demandes avec journalisation des accès au serveur.

Envisagez également de mettre en œuvre des contrôles de détection continus à l'aide de la règle s3-bucket-logging-enabled AWS Config gérée.

Utilisez AWS CloudTrail

AWS CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS dans Amazon S3. Vous pouvez utiliser les informations collectées par CloudTrail pour déterminer les éléments suivants :

- La demande qui a été adressée à Amazon S3
- L'adresse IP à partir de laquelle la demande a été effectuée
- La personne ayant effectué la demande
- La date et l'heure où la demande a été effectuée
- Des détails supplémentaires sur la demande

Par exemple, vous pouvez identifier les CloudTrail entrées pour les PUT actions qui affectent l'accès aux données`PutBucketAcl`, en particulier`PutObjectAcl`,`PutBucketPolicy`, et`PutBucketWebsite`.

Lorsque vous configurez votre Compte AWS, CloudTrail est activé par défaut. Vous pouvez consulter les événements récents dans la CloudTrail console. Pour créer un enregistrement continu de l'activité et des événements de vos compartiments Amazon S3, vous pouvez créer un suivi dans la CloudTrail console. Pour plus d'informations, consultez Journalisation des événements de données dans le Guide de l'utilisateur AWS CloudTrail .

Lorsque vous créez un suivi, vous pouvez le configurer CloudTrail pour consigner les événements liés aux données. Les événements de données sont des enregistrements d'opérations de ressources effectuées sur ou dans une ressource. Dans Amazon S3, les événements de données enregistrent l'activité de l'API au niveau de l'objet pour des compartiments individuels. CloudTrail prend en charge un sous-ensemble d'opérations d'API au niveau des objets Amazon

S3, telles que`GetObject`, et`DeleteObject`. `PutObject` Pour plus d'informations sur le CloudTrail fonctionnement d'Amazon S3, consultezJournalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail. Dans la console Amazon S3, vous pouvez également configurer vos compartiments S3 pour Activation de la journalisation des CloudTrail événements pour les compartiments et les objets S3.

AWS Config fournit une règle gérée (`cloudtrail-s3-dataevents-enabled`) que vous pouvez utiliser pour vérifier qu'au moins un journal CloudTrail enregistre des événements de données pour vos compartiments S3. Pour plus d'informations, consultez cloudtrail-s3-dataevents-enabled dans le Guide du développeur AWS Config .

Activer AWS Config

Plusieurs des meilleures pratiques répertoriées dans cette rubrique suggèrent de créer des AWS Config règles. AWS Config vous aide à évaluer, auditer et évaluer les configurations de vos AWS ressources. AWS Config surveille les configurations des ressources afin que vous puissiez évaluer les configurations enregistrées par rapport aux configurations sécurisées souhaitées. Avec AWS Config, vous pouvez effectuer les opérations suivantes :

- Examiner les modifications apportées aux configurations et aux relations entre les ressources AWS
- Suivre les historiques détaillés de la configuration des ressources
- Déterminer votre conformité globale face aux configurations spécifiées dans vos instructions internes

Son utilisation AWS Config peut vous aider à simplifier l'audit de conformité, l'analyse de sécurité, la gestion des modifications et le dépannage opérationnel. Pour plus d'informations, consultez la section Configuration AWS Config avec la console dans le guide du AWS Config développeur. Lors de la spécification des types de ressources à enregistrer, assurez-vous d'inclure les ressources Amazon S3.

> **Important**
>
> AWS Config les règles gérées ne prennent en charge que les compartiments à usage général lors de l'évaluation des ressources Amazon S3. AWS Config n'enregistre pas les modifications de configuration pour les compartiments de répertoire. Pour plus d'informations, consultez les AWS Config sections Règles gérées et Liste des règles AWS Config gérées dans le Guide du AWS Config développeur.

Pour un exemple d'utilisation AWS Config, consultez Comment utiliser AWS Config pour surveiller et répondre aux compartiments Amazon S3 autorisant un accès public sur le blog sur la AWS sécurité.

Utilisation de S3 Storage Lens

S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. S3 Storage Lens analyse également les métriques de stockage pour fournir des recommandations contextuelles afin d'aider à réduire les coûts de stockage et à appliquer les bonnes pratiques de protection des données.

Avec S3 Storage Lens, vous pouvez utiliser des métriques pour générer des informations récapitulatives, telles que la quantité de stockage dont vous disposez dans l'ensemble de votre organisation ou les compartiments et préfixes qui connaissent la croissance la plus rapide. Vous pouvez également utiliser les métriques S3 Storage Lens pour identifier des opportunités d'optimisation des coûts, mettre en œuvre les bonnes pratiques de protection des données et de gestion des accès, et améliorer les performances des charges de travail d'application.

Par exemple, vous pouvez identifier les compartiments qui sont dépourvus de règles de cycle de vie S3 pour abandonner les chargements partitionnés non terminés datant de plus de 7 jours. Vous pouvez également identifier les compartiments qui ne respectent pas les bonnes pratiques de protection des données, telles que l'utilisation de la réplication S3 ou de la gestion des versions S3. Pour plus d'informations, consultez Présentation d'Amazon S3 Storage Lens.

Surveillance des conseils de sécurité AWS

Nous vous recommandons de vérifier régulièrement les conseils de sécurité publiés dans Trusted Advisor pour votre Compte AWS. En particulier, recherchez des avertissements concernant les compartiments Amazon S3 avec des autorisations permettant un libre accès. Vous pouvez procéder par programmation en utilisant describe-trusted-advisor-checks.

De plus, surveillez activement l'adresse e-mail principale enregistrée pour chacun de vos Comptes AWS. AWS utilise cette adresse e-mail pour vous contacter au sujet de problèmes de sécurité émergents susceptibles de vous affecter.

AWS les problèmes opérationnels ayant un large impact sont publiés sur le site AWS Health Dashboard - Santé du service. Les problèmes opérationnels sont également publiés dans les comptes individuels via le tableau de bord AWS Health Dashboard. Pour plus d'informations, consultez la documentation AWS Health.

Surveillance de la sécurité des données à l'aide AWS de services de sécurité gérés

Plusieurs services AWS de sécurité gérés peuvent vous aider à identifier, évaluer et surveiller les risques de sécurité et de conformité pour vos données Amazon S3. Ils peuvent également vous aider à protéger vos données contre ces risques. Ces services incluent des fonctionnalités de détection, de surveillance et de protection automatisées conçues pour passer des ressources Amazon S3 individuelles Compte AWS aux ressources destinées aux entreprises comptant des milliers de personnes Comptes AWS.

AWS les services de détection et de réponse peuvent vous aider à identifier les erreurs de configuration de sécurité, les menaces ou les comportements inattendus potentiels, afin que vous puissiez réagir rapidement à des activités potentiellement non autorisées ou malveillantes dans votre environnement. AWS les services de protection des données peuvent vous aider à surveiller et à protéger vos données, vos comptes et vos charges de travail contre tout accès non autorisé. Ils peuvent également vous aider à découvrir des données sensibles, telles que des données d'identification personnelle (PII), dans votre parc de données Amazon S3.

Pour vous aider à identifier et à évaluer les risques liés à la sécurité et à la conformité des données, les services de sécurité AWS gérés génèrent des résultats pour vous informer des événements ou des problèmes de sécurité potentiels liés à vos données Amazon S3. Ces résultats fournissent des informations pertinentes qui vous serviront à étudier et évaluer ces risques et à y réagir en fonction de vos flux de travail et de vos politiques de réponse aux incidents. Vous pouvez accéder directement aux données des résultats en utilisant chaque service. Vous pouvez également envoyer les données à d'autres applications, services et systèmes, tels que votre système de gestion des incidents et des événements de sécurité (SIEM).

Pour surveiller la sécurité de vos données Amazon S3, pensez à utiliser ces services AWS de sécurité gérés.

Amazon GuardDuty

Amazon GuardDuty est un service de détection des menaces qui surveille en permanence votre activité Comptes AWS et votre charge de travail pour détecter toute activité malveillante et fournit des résultats de sécurité détaillés à des fins de visibilité et de correction.

Avec la fonctionnalité de protection S3 intégrée GuardDuty, vous pouvez configurer GuardDuty pour analyser les événements AWS CloudTrail de gestion et de données relatifs à vos ressources Amazon S3. GuardDuty surveille ensuite ces événements pour détecter toute activité malveillante

et suspecte. Pour éclairer l'analyse et identifier les risques de sécurité potentiels, GuardDuty utilise des flux de renseignements sur les menaces et l'apprentissage automatique.

GuardDuty peut surveiller différents types d'activité pour vos ressources Amazon S3. Par exemple, les événements CloudTrail de gestion pour Amazon S3 incluent des opérations au niveau du compartiment, telles que `ListBuckets`et. `DeleteBucket` `PutBucketReplication` CloudTrail les événements de données pour Amazon S3 incluent des opérations au niveau des objets, telles que `GetObject`et. `ListObjects` `PutObject` S'il GuardDuty détecte une activité anormale ou potentiellement malveillante, il génère une constatation pour vous en informer.

Pour plus d'informations, consultez Amazon S3 Protection dans Amazon GuardDuty dans le guide de GuardDuty l'utilisateur Amazon.

Amazon Detective

Amazon Detective simplifie le processus d'investigation et vous aide à mener des investigations de sécurité plus rapides et plus efficaces. Detective fournit des agrégations de données, des résumés et un contexte prédéfinis qui peuvent vous aider à analyser et à évaluer la nature et l'étendue des éventuels problèmes de sécurité.

Detective extrait automatiquement les événements temporels, tels que les appels d'API AWS CloudTrail et les journaux de flux Amazon VPC pour AWS vos ressources. Il ingère également les résultats générés par Amazon GuardDuty. Detective utilise ensuite le machine learning, l'analyse statistique et la théorie des graphes pour générer des visualisations qui vous aideront à mener plus rapidement des investigations de sécurité efficaces.

Ces visualisations fournissent une vue unifiée et interactive des comportements des ressources et de leurs interactions au fil du temps. Vous pouvez explorer ce graphique de comportement pour examiner les actions potentiellement malveillantes, telles que les tentatives de connexion infructueuses ou les appels d'API suspects. Vous pouvez également voir comment ces actions affectent les ressources, notamment les objets et les compartiments S3.

Pour plus d'informations, consultez le Guide d'administration Amazon Detective.

IAM Access Analyzer

AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) peut vous aider à identifier les ressources partagées avec une entité externe. Vous pouvez également utiliser IAM Access Analyzer pour valider les politiques IAM par rapport à la grammaire des politiques et

aux meilleures pratiques, et générer des politiques IAM en fonction de l'activité d'accès dans vos journaux. AWS CloudTrail

IAM Access Analyzer utilise un raisonnement basé sur la logique pour analyser les politiques de ressources de votre AWS environnement, telles que les politiques relatives aux compartiments. Avec IAM Access Analyzer pour S3, vous êtes alerté lorsqu'un compartiment S3 est configuré pour autoriser l'accès à toute personne sur Internet ou autre Comptes AWS, y compris à des comptes extérieurs à votre organisation. Par exemple, l'analyseur d'accès IAM pour S3 peut signaler qu'un compartiment dispose d'un accès en lecture ou en écriture fourni via une liste de contrôle d'accès (ACL) de compartiment, une politique de compartiment, une politique de point d'accès multirégion ou une politique de point d'accès. Pour chaque compartiment public ou partagé, vous recevez des résultats qui indiquent la source et le niveau d'accès public ou partagé. Grâce à ces résultats, vous pouvez prendre des mesures correctives immédiates et précises pour restaurer l'accès au compartiment comme vous l'aviez prévu.

Pour plus d'informations, consultez Examen de l'accès aux compartiments à l'aide de l'analyseur d'accès IAM pour S3.

Amazon Macie

Amazon Macie est un service de sécurité qui découvre les données sensibles au moyen du machine learning et de la correspondance de modèles. Macie fournit une visibilité sur les risques liés à la sécurité des données et permet une protection automatisée contre ces risques. Grâce à Macie, vous pouvez automatiser la découverte et la création de rapports de données sensibles dans votre parc de données Amazon S3 afin de mieux comprendre les données stockées par votre organisation dans S3.

Pour détecter les données sensibles avec Macie, vous pouvez utiliser des critères et des techniques intégrés, conçus pour détecter une liste étendue et croissante de types de données sensibles pour de nombreux pays et régions. Ces types de données sensibles incluent plusieurs types de données d'identification personnelle (PII), des données financières et des informations d'identification. Vous pouvez également utiliser des critères personnalisés que vous définissez : des expressions régulières qui définissent des modèles de texte à mettre en correspondance et, éventuellement, des séquences de caractères et des règles de proximité pour affiner les résultats.

Si Macie détecte des données sensibles dans un objet S3, Macie génère un résultat de sécurité pour vous en informer. Ce résultat fournit des informations sur l'objet affecté, les types et le nombre d'occurrences des données sensibles découvertes par Macie, ainsi que des détails supplémentaires pour vous aider à mener des investigations sur le compartiment et l'objet S3 affectés. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon Macie.

AWS Security Hub

AWS Security Hub est un service de gestion de la posture de sécurité qui effectue des vérifications des meilleures pratiques de sécurité, regroupe les alertes et les résultats provenant de sources multiples dans un format unique et permet des mesures correctives automatisées.

Security Hub collecte et fournit des données relatives aux résultats de AWS Partner Network sécurité à partir de solutions de sécurité intégrées Services AWS, notamment Amazon Detective, Amazon GuardDuty, IAM Access Analyzer et Amazon Macie. Il génère également ses propres conclusions en effectuant des contrôles de sécurité continus et automatisés basés sur les AWS meilleures pratiques et les normes du secteur prises en charge.

Security Hub met ensuite en corrélation et consolide les résultats entre les fournisseurs, afin de vous aider à hiérarchiser et à traiter les résultats les plus significatifs. Il prend également en charge les actions personnalisées, que vous pouvez utiliser pour invoquer des réponses ou des actions de correction pour des classes spécifiques de résultats.

Avec Security Hub, vous pouvez évaluer l'état de sécurité et de conformité de vos ressources Amazon S3, dans le cadre d'une analyse plus large du niveau de sécurité de votre entreprise au niveau individuel Régions AWS et dans plusieurs régions. Cela inclut l'analyse des tendances en matière de sécurité et l'identification des problèmes de sécurité prioritaires. Vous pouvez également agréger les résultats de plusieurs Régions AWS, ainsi que surveiller et traiter les données de résultats agrégées provenant d'une seule région.

Pour plus d'informations, consultez Contrôles Amazon Simple Storage Service dans le Guide de l'utilisateur AWS Security Hub .

Protection des données dans Amazon S3

Simple Storage Service (Amazon S3) offre une infrastructure de stockage hautement durable, pensée pour le stockage de données primaires et stratégiques. S3 standard, S3 Intelligent-Tiering, S3 standard – Accès peu fréquent, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive stockent des objets de façon redondante sur plusieurs appareils sur un minimum de trois zones de disponibilité dans une Région AWS. Une zone de disponibilité est un ou plusieurs centres de données discrets dotés d'une alimentation, d'un réseau et d'une connectivité redondants dans une Région AWS. Les zones de disponibilité sont physiquement séparées par une distance significative, de plusieurs kilomètres, de toute autre zone de disponibilité, bien qu'elles se trouvent toutes à moins de 100 km (60 miles) les unes des autres. La classe de

stockage S3 One Zone-IA stocke les données de façon redondante sur plusieurs appareils au sein d'une seule zone de disponibilité. Ces services sont conçus pour gérer les défaillances de périphériques concurrents en détectant et en réparant rapidement toute redondance perdue, et ils vérifient également régulièrement l'intégrité de vos données à l'aide de totaux de contrôle.

Le stockage Amazon S3 Standard présente les caractéristiques suivantes :

- Soutenu par le contrat de niveau de service (SLA) Amazon S3.
- Conçu pour fournir une 99,999999999 % de durabilité et 99,99 % de disponibilité des objets sur une année donnée.
- S3 standard, S3 Intelligent-Tiering, S3 standard – Accès peu fréquent, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive sont tous conçus pour garder les données en cas de perte d'une zone de disponibilité Amazon S3 complète.

Simple Storage Service (Amazon S3) protège également vos données à l'aide de la gestion des versions. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. Le contrôle de version permet de récupérer facilement les données en cas d'actions involontaires des utilisateurs ou de défaillances des applications. Par défaut, les demandes récupèrent la version écrite la plus récente. Vous pouvez récupérer les versions antérieures d'un objet en spécifiant une version de l'objet dans une demande.

Outre la gestion des versions S3, vous pouvez également utiliser le verrouillage d'objets Amazon S3 et la réplication S3 pour protéger vos données. Pour de plus amples informations, veuillez consulter Protection des données dans Amazon S3.

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer des comptes utilisateur individuels AWS Identity and Access Management, afin que chaque utilisateur ne dispose que des autorisations nécessaires pour accomplir ses tâches.

Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 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 (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Les bonnes pratiques de sécurité suivantes s'appliquent également à la protection des données dans Amazon S3 :

- Implement server-side encryption
- Enforce encryption of data in transit
- Consider using Macie with Amazon S3
- Identify and audit all your Amazon S3 buckets
- Monitor Amazon Web Services security advisories

Protection des données à l'aide du chiffrement

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

La protection des données fait référence à la protection des données pendant que celles-ci sont en transit (à destination ou en provenance d'Amazon S3) et au repos (durant leur stockage sur les disques de centres de données Amazon S3). Vous pouvez protéger les données en transit en utilisant le protocole Secure Socket Layer/Transport Layer Security (SSL/TLS) ou le chiffrement côté client. Pour protéger des données au repos dans Amazon S3, vous disposer des options suivantes :

- Chiffrement côté serveur : Amazon S3 chiffre vos objets avant de les enregistrer sur des disques dans des centres de AWS données, puis les déchiffre lorsque vous les téléchargez.

  Le chiffrement est configuré par défaut pour tous les compartiments Amazon S3, et tous les nouveaux objets qui sont chargés dans un compartiment S3 sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment dans Amazon S3. Pour utiliser un autre type de chiffrement, vous pouvez soit spécifier le type de chiffrement côté serveur à

utiliser dans vos PUT demandes S3, soit mettre à jour la configuration de chiffrement par défaut dans le compartiment de destination.

Si vous souhaitez spécifier un type de chiffrement différent dans vos PUT demandes, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), le chiffrement double couche côté serveur avec des clés (DSSE-KMS) ou le chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C). Si vous souhaitez définir une autre configuration de chiffrement par défaut dans le compartiment de destination, vous pouvez utiliser SSE-KMS ou DSSE-KMS.

Pour plus d'informations sur la modification de la configuration de chiffrement par défaut pour vos compartiments à usage général, consultezConfiguration du chiffrement par défaut.

Lorsque vous modifiez la configuration de chiffrement par défaut de votre compartiment en SSE-KMS, le type de chiffrement des objets Amazon S3 existants dans le compartiment n'est pas modifié. Pour modifier le type de chiffrement de vos objets préexistants après avoir mis à jour la configuration de chiffrement par défaut vers SSE-KMS, vous pouvez utiliser Amazon S3 Batch Operations. Vous fournissez à S3 Batch Operations une liste d'objets, et Batch Operations appelle l'opération d'API correspondante. Vous pouvez utiliser cette Copie d'objets action pour copier des objets existants, ce qui les réécrit dans le même compartiment que les objets chiffrés SSE-KMS. Une tâche d'opérations par lots peut effectuer l'opération spécifiée sur des milliards d'objets. Pour plus d'informations, consultez Exécution d'opérations groupées sur des objets avec les opérations par lot le billet de blog sur le AWS stockage Comment chiffrer rétroactivement des objets existants dans Amazon S3 à l'aide de S3 Inventory, Amazon Athena et S3 Batch Operations.

Pour plus d'informations sur chaque option pour le chiffrement côté serveur, consultez Protection des données avec le chiffrement côté serveur.

Pour configurer le chiffrement côté serveur, consultez :

- Spécification du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
- Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS)
- the section called "Spécification de DSSE-KMS"
- Spécification du chiffrement côté serveur avec des clés fournies par le client (SSE-C)

- Chiffrement côté client : vous chiffrez vos données côté client et chargez les données chiffrées dans Amazon S3. Dans ce cas, vous gérez le processus de chiffrement, les clés de chiffrement et les outils associés.

Pour configurer le chiffrement côté client, consultez Protection des données avec le chiffrement côté client.

Pour savoir quel pourcentage de vos octets de stockage sont chiffrés, vous pouvez utiliser les métriques Amazon S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Pour plus d'informations, consultez Évaluer l'activité et l'utilisation de votre stockage avec S3 Storage Lens. Pour obtenir la liste complète des métriques, consultez le Glossaire des métriques S3 Storage Lens.

Pour plus d'informations sur le chiffrement côté serveur et le chiffrement côté client, consultez les rubriques suivantes.

Rubriques

- Protection des données avec le chiffrement côté serveur
- Protection des données avec le chiffrement côté client

Protection des données avec le chiffrement côté serveur

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Le chiffrement côté serveur est le chiffrement des données à leur destination par l'application ou le service qui les reçoit. Amazon S3 chiffre vos données au niveau de l'objet lorsqu'il les écrit sur les disques des centres de AWS données et les déchiffre pour vous lorsque vous y accédez. Tant

que vous authentifiez votre demande et que vous avez des autorisations d'accès, il n'y a aucune différence dans la manière dont vous accédez aux objets chiffrés ou déchiffrés. Par exemple, si vous partagez vos objets en utilisant une URL pré-signée, cette URL fonctionne de la même manière pour les objets chiffrés et déchiffrés. En outre, quand vous répertoriez les objets de votre compartiment, les opérations d'API de liste renvoient la liste de tous les objets, qu'ils soient chiffrés ou non.

Le chiffrement est configuré par défaut pour tous les compartiments Amazon S3, et tous les nouveaux objets qui sont chargés dans un compartiment S3 sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment dans Amazon S3. Pour utiliser un autre type de chiffrement, vous pouvez soit spécifier le type de chiffrement côté serveur à utiliser dans vos PUT demandes S3, soit mettre à jour la configuration de chiffrement par défaut dans le compartiment de destination.

Si vous souhaitez spécifier un type de chiffrement différent dans vos PUT demandes, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), le chiffrement double couche côté serveur avec des clés (DSSE-KMS) ou le chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C). Si vous souhaitez définir une autre configuration de chiffrement par défaut dans le compartiment de destination, vous pouvez utiliser SSE-KMS ou DSSE-KMS.

Pour plus d'informations sur la modification de la configuration de chiffrement par défaut pour vos compartiments à usage général, consultezConfiguration du chiffrement par défaut.

Lorsque vous modifiez la configuration de chiffrement par défaut de votre compartiment en SSE-KMS, le type de chiffrement des objets Amazon S3 existants dans le compartiment n'est pas modifié. Pour modifier le type de chiffrement de vos objets préexistants après avoir mis à jour la configuration de chiffrement par défaut vers SSE-KMS, vous pouvez utiliser Amazon S3 Batch Operations. Vous fournissez à S3 Batch Operations une liste d'objets, et Batch Operations appelle l'opération d'API correspondante. Vous pouvez utiliser cette Copie d'objets action pour copier des objets existants, ce qui les réécrit dans le même compartiment que les objets chiffrés SSE-KMS. Une tâche d'opérations par lots peut effectuer l'opération spécifiée sur des milliards d'objets. Pour plus d'informations, consultez Exécution d'opérations groupées sur des objets avec les opérations par lot le billet de blog sur le AWS stockage Comment chiffrer rétroactivement des objets existants dans Amazon S3 à l'aide de S3 Inventory, Amazon Athena et S3 Batch Operations.

> **Note**
>
> Vous ne pouvez pas appliquer simultanément différents types de chiffrement côté serveur au même objet.

Si vous devez chiffrer vos objets existants, utilisez S3 Batch Operations et S3 Inventory. Pour plus d'informations, consultez Encrypting objects with Amazon S3 Batch Operations (Chiffrement d'objets avec des opérations par lot Amazon S3) et Exécution d'opérations groupées sur des objets avec les opérations par lot.

Lorsque vous stockez des données dans Amazon S3, vous disposez de quatre options de chiffrement côté serveur qui s'excluent mutuellement, en fonction de la façon dont vous choisissez de gérer les clés de chiffrement et du nombre de couches de chiffrement que vous souhaitez appliquer.

Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

Le chiffrement est configuré par défaut pour tous les compartiments Amazon S3. L'option par défaut pour le chiffrement côté serveur est avec des clés gérées Amazon S3 (SSE-S3). Chaque objet est chiffré à l'aide d'une clé unique. Comme protection supplémentaire, SSE-S3 chiffre la clé elle-même à l'aide d'une clé racine dont il effectue une rotation régulière. SSE-S3 utilise l'un des chiffrements par bloc les plus puissants qui existent, Advanced Encryption Standard 256 bits (AES-256), pour chiffrer vos données. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

Chiffrement côté serveur avec clés AWS Key Management Service (AWS KMS) (SSE-KMS)

Le chiffrement côté serveur avec AWS KMS keys (SSE-KMS) est fourni par le biais d'une intégration du service à AWS KMS Amazon S3. Avec AWS KMS, vous avez plus de contrôle sur vos clés. Par exemple, vous pouvez afficher des clés distinctes, modifier des politiques de contrôle et suivre les clés dans AWS CloudTrail. En outre, vous pouvez créer et gérer les clés gérées par le client ou utiliser les Clés gérées par AWS qui sont propres à vous-même, à votre service et à votre région. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

Chiffrement double couche côté serveur avec clés AWS Key Management Service (AWS KMS) (DSSE-KMS)

Le chiffrement double couche côté serveur avec AWS KMS keys (DSSE-KMS) est similaire au SSE-KMS, mais le DSSE-KMS applique deux couches individuelles de chiffrement au niveau des

objets au lieu d'une seule couche. Les deux couches de chiffrement étant appliquées à un objet côté serveur, vous pouvez utiliser un large éventail d' Services AWS outils pour analyser les données dans S3 tout en utilisant une méthode de chiffrement répondant à vos exigences de conformité. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement double couche côté serveur avec AWS KMS clés (DSSE-KMS).

Chiffrement côté serveur avec clés fournies par le client (SSE-C)

Dans le cadre du chiffrement côté serveur avec des clés fournies par le client (SSE-C), vous gérez les clés de chiffrement, et Amazon S3 gère le chiffrement à mesure qu'il écrit les données sur les disques et le déchiffrement au moment où vous accédez à vos objets. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur avec les clés fournies par le client (SSE-C).

> **Note**
>
> Lorsque vous utilisez des points d'accès pour les systèmes de FSx fichiers Amazon à l'aide de points d'accès S3, vous disposez d'une option pour le chiffrement côté serveur.
>
> Chiffrement côté serveur avec Amazon FSx (SSE-FSX)
>
> Le chiffrement de tous les systèmes de FSx fichiers Amazon est configuré par défaut et sont chiffrés au repos à l'aide de clés gérées à l'aide de AWS Key Management Service. Les données sont automatiquement cryptées et déchiffrées par le système de fichiers au fur et à mesure que les données sont écrites et lues dans le système de fichiers. Ces processus sont gérés de manière transparente par Amazon FSx.

Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans

AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Tous les compartiments Amazon S3 ont le chiffrement configuré par défaut et les objets sont automatiquement chiffrés à l'aide du chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3). Ce paramètre de chiffrement s'applique à tous les objets de vos compartiments Amazon S3.

Si vous avez besoin d'un contrôle accru sur vos clés, par exemple pour gérer la rotation des clés et les autorisations de politique d'accès, vous pouvez choisir d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) ou le chiffrement côté serveur à double couche avec clés (DSSE-KMS). AWS KMS Pour en savoir plus sur la modification des clés KMS, consultez Modification des clés dans le Guide du développeur AWS Key Management Service .

Note

Nous avons modifié les compartiments afin de chiffrer automatiquement les nouveaux chargements d'objets. Si vous avez déjà créé un compartiment sans chiffrement par défaut, Amazon S3 activera le chiffrement par défaut pour le compartiment à l'aide de SSE-S3. Aucune modification ne sera apportée à la configuration de chiffrement par défaut d'un compartiment existant pour lequel le chiffrement SSE-S3 ou SSE-KMS est déjà configuré. Si vous souhaitez chiffrer vos objets avec SSE-KMS, vous devez modifier le type de chiffrement dans les paramètres de votre compartiment. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

Lorsque vous configurez votre compartiment pour utiliser le chiffrement par défaut avec SSE-KMS, vous pouvez également activer les clés de compartiment S3 afin de réduire le trafic de demandes en provenance d'Amazon S3 AWS KMS et de réduire le coût du chiffrement. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

Pour identifier les compartiments dont le chiffrement par défaut est activé par SSE-KMS, vous pouvez utiliser les métriques Amazon S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation

sur l'utilisation et l'activité du stockage d'objets. Pour plus d'informations, consultez Utilisation de S3 Storage Lens pour protéger vos données.

Lorsque vous utilisez le chiffrement côté serveur, Amazon S3 chiffre un objet avant de l'enregistrer sur disque et le déchiffre lorsque vous téléchargez l'objet. Pour plus d'informations sur la protection des données à l'aide du chiffrement côté serveur et de la gestion des clés de chiffrement, consultez Protection des données avec le chiffrement côté serveur.

Pour en savoir plus sur les autorisations nécessaires pour le chiffrement par défaut, consultez PutBucketEncryption dans la documentation de référence de l'API Amazon Simple Storage Service.

Vous pouvez configurer le comportement de chiffrement par défaut d'Amazon S3 pour un compartiment S3 à l'aide de la console Amazon S3, de l'API REST Amazon S3 et de l'interface de ligne de AWS commande (AWS CLI). AWS SDKs

Chiffrement des objets existants

Pour chiffrer vos objets Amazon S3 non chiffrés existants, vous pouvez utiliser des opérations par lot Amazon S3. Vous fournissez à la fonctionnalité d'opérations par lots S3 une liste d'objets sur lesquels agir. La fonctionnalité d'opérations par lots appelle l'API correspondante pour exécuter l'opération spécifiée. Vous pouvez utiliser l'opération de copie des opérations par lot pour copier des objets non chiffrés et les réécrire dans le même compartiment en tant qu'objets chiffrés. Une tâche d'opérations par lots peut effectuer l'opération spécifiée sur des milliards d'objets. Pour plus d'informations, consultez Exécution d'opérations groupées sur des objets avec les opérations par lot et le billet de blog sur le stockage AWS intitulé Encrypting objects with Amazon S3 Batch Operations.

Vous pouvez également chiffrer des objets existants à l'aide de l'opération `CopyObject` API ou de la `copy-object` AWS CLI commande. Pour plus d'informations, consultez le billet de blog sur le stockage AWS intitulé Encrypting existing Amazon S3 objects with the AWS CLI.

> **Note**
>
> Les compartiments Amazon S3 pour lesquels le chiffrement de compartiment par défaut est défini sur SSE-KMS ne peuvent pas servir de compartiments de destination pour the section called "Enregistrement de l'accès au serveur". Seul le chiffrement par défaut SSE-S3 est pris en charge pour les compartiments de destination du journal d'accès au serveur.

Utilisation du chiffrement SSE-KMS pour les opérations intercomptes

Tenez compte des éléments suivants lors de l'utilisation du chiffrement pour les opérations inter-comptes :

- Si aucun nom de ressource AWS KMS key Amazon (ARN) ou alias n'est fourni au moment de la demande ou via la configuration de chiffrement par défaut du bucket, le Clé gérée par AWS (`aws/s3`) est utilisé.
- Si vous téléchargez ou accédez à des objets S3 à l'aide de principes AWS Identity and Access Management (IAM) identiques Compte AWS à ceux de votre clé KMS, vous pouvez utiliser le Clé gérée par AWS (). `aws/s3`
- Utilisez une clé gérée par le client si vous souhaitez accorder un accès intercompte à vos objets S3. Vous pouvez configurer la politique d'une clé gérée par le client afin d'autoriser l'accès à partir d'un autre compte.
- Si vous spécifiez une clé KMS gérée par le client, nous recommandons d'utiliser un ARN de clé KMS complet. Si vous utilisez plutôt un alias de clé KMS, AWS KMS la clé est résolue dans le compte du demandeur. En raison de ce comportement, les données peuvent être chiffrées avec une clé KMS qui appartient au demandeur, et non au propriétaire du compartiment.
- Vous devez spécifier une clé pour laquelle vous (le demandeur) avez obtenu l'autorisation de `Encrypt`. Pour en savoir plus, consultez Permettre aux utilisateurs de clés d'utiliser une clé KMS pour les opérations de chiffrement dans le Guide de l'utilisateur AWS Key Management Service .

Pour plus d'informations sur les circonstances dans lesquelles utiliser des clés gérées par le client et des clés KMS AWS gérées, consultez Dois-je utiliser une clé gérée par le client Clé gérée par AWS ou une clé gérée par le client pour chiffrer mes objets dans Amazon S3 ?

Utilisation du chiffrement par défaut avec la réplication

Après avoir activé le chiffrement par défaut pour un compartiment de destination de réplication, le comportement de chiffrement suivant s'applique :

- Si des objets du compartiment source ne sont pas chiffrés, les objets réplica du compartiment de destination sont chiffrés à l'aide des paramètres de chiffrement par défaut du compartiment de destination. Par conséquent, les étiquettes d'entité (ETags) des objets sources sont différentes de celles ETags des objets répliqués. Si certaines applications l'utilisent ETags, vous devez les mettre à jour pour tenir compte de cette différence.

- Si les objets du compartiment source sont chiffrés à l'aide d'un chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3), d'un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) ou d'un chiffrement double couche côté serveur avec AWS KMS clés (DSSE-KMS), les objets répliques du compartiment de destination utilisent le même type de chiffrement que les objets source. Les paramètres de chiffrement par défaut du compartiment de destination ne sont pas utilisés.

Pour plus d'informations sur l'utilisation du chiffrement par défaut avec SSE-KMS, consultez Réplication d'objets chiffrés.

Utilisation des clés de compartiment Amazon S3 avec chiffrement par défaut

Lorsque vous configurez votre compartiment pour utiliser SSE-KMS comme le comportement de chiffrement par défaut sur de nouveaux objets, vous pouvez également configurer des clés de compartiment S3. Les clés de compartiment S3 réduisent le nombre de transactions depuis Amazon S3 AWS KMS afin de réduire le coût du SSE-KMS.

Lorsque vous configurez votre compartiment pour utiliser les clés de compartiment S3 pour SSE-KMS sur de nouveaux objets, il AWS KMS génère une clé au niveau du compartiment qui est utilisée pour créer une clé de données unique pour les objets du compartiment. Cette clé de compartiment S3 est utilisée pendant une période limitée dans le temps dans Amazon S3, ce qui réduit la nécessité pour Amazon S3 de faire des demandes AWS KMS pour effectuer des opérations de chiffrement.

Pour plus d'informations sur l'utilisation des clés de compartiment S3, consultez Utilisation de clés de compartiment Amazon S3..

Configuration du chiffrement par défaut

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line

Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Les compartiments Amazon S3 ont le chiffrement des compartiments activé par défaut et les nouveaux objets sont automatiquement chiffrés à l'aide du chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3). Ce chiffrement s'applique à tous les nouveaux objets de vos compartiments Amazon S3, sans frais.

Si vous avez besoin d'un contrôle accru sur vos clés de chiffrement, par exemple pour gérer la rotation des clés et l'attribution des politiques d'accès, vous pouvez choisir d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) ou le chiffrement côté serveur à double couche avec clés (DSSE-KMS). AWS KMS Pour en savoir plus sur SSE-KMS, consultez Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS). Pour en savoir plus sur DSSE-KMS, consultez the section called "Chiffrement double couche côté serveur (DSSE-KMS)".

Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez avoir l'autorisation d'utiliser la clé. Pour plus d'informations sur les autorisations intercomptes pour les clés KMS, consultez Création de clés KMS que d'autres comptes peuvent utiliser dans le Guide du développeur AWS Key Management Service .

Lorsque vous définissez le chiffrement de compartiment par défaut sur SSE-KMS, vous pouvez également configurer une clé de compartiment S3 afin de réduire les coûts de vos AWS KMS demandes. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

> **Note**
>
> Si vous avez l'habitude PutBucketEncryptionde définir le chiffrement de votre compartiment par défaut sur SSE-KMS, vous devez vérifier que l'ID de votre clé KMS est correct. Amazon S3 ne valide pas l'ID de clé KMS fourni dans les PutBucketEncryption demandes.

Il n'y a pas de frais supplémentaires relatifs à l'utilisation du chiffrement par défaut pour les compartiments S3. Les demandes de configuration du comportement de chiffrement par défaut seront facturées comme des demandes Amazon S3 standard. Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3. Pour le SSE-KMS et le DSSE-KMS, des AWS KMS frais s'appliquent et sont indiqués dans le prix.AWS KMS

Le chiffrement côté serveur avec des clés fournies par le client (SSE-C) n'est pas pris en charge pour le chiffrement par défaut.

Vous pouvez configurer le chiffrement par défaut d'Amazon S3 pour un compartiment S3 à l'aide de la console Amazon S3 AWS SDKs, de l'API REST Amazon S3 et du AWS Command Line Interface (AWS CLI).

Modifications à prendre en compte avant d'activer le chiffrement par défaut

Après avoir activé le chiffrement par défaut pour un compartiment, le comportement de chiffrement suivant s'applique :

- Il n'y a pas de modification pour le chiffrement des objets qui existaient dans le compartiment avant l'activation du chiffrement par défaut.
- Lorsque vous chargez des objets après l'activation du chiffrement par défaut :
  - Si vos en-têtes de demandes PUT ne comportent pas d'informations de chiffrement, Amazon S3 utilise les paramètres de chiffrement par défaut du compartiment pour chiffrer les objets.
  - Si vos en-têtes de demandes PUT comportent des informations de chiffrement, Amazon S3 utilise les informations de la demande PUT pour chiffrer les objets avant de les stocker dans Amazon S3.
- Si vous utilisez l'option SSE-KMS ou DSSE-KMS pour votre configuration du chiffrement par défaut, vous êtes soumis aux quotas RPS (demandes par seconde) de AWS KMS. Pour plus d'informations sur les quotas de AWS KMS et sur la procédure à suivre pour demander une augmentation des quotas, consultez Quotas dans le Guide du développeur AWS Key Management Service .

> **Note**
>
> Les objets chargés avant l'activation du chiffrement par défaut ne seront pas chiffrés. Pour plus d'informations sur le chiffrement d'objets existants, consultez the section called "Définition du chiffrement du compartiment par défaut".

Utilisation de la console S3

Pour configurer le chiffrement par défaut sur un compartiment Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment que vous souhaitez utiliser.
4. Choisissez l'onglet Propriétés.
5. Sous Default encryption (Chiffrement par défaut), choisissez Edit (Modifier).
6. Pour configurer le chiffrement, sous Type de chiffrement, choisissez l'une des options suivantes :

   - Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
   - Chiffrement côté serveur avec AWS Key Management Service clés (SSE-KMS)
   - Chiffrement double couche côté serveur avec AWS Key Management Service clés (DSSE-KMS)

   > **Important**
   >
   > Si vous utilisez l'option SSE-KMS ou DSSE-KMS pour votre configuration du chiffrement par défaut, vous êtes soumis aux quotas RPS (demandes par seconde) de AWS KMS. Pour plus d'informations sur les AWS KMS quotas et sur la manière de demander une augmentation de quota, consultez la section Quotas dans le guide du AWS Key Management Service développeur.

   Les compartiments et les nouveaux objets sont chiffrés par défaut avec SSE-S3, sauf si vous spécifiez un autre type de chiffrement par défaut pour vos compartiments. Pour plus d'informations sur le chiffrement par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.

   Pour en savoir plus sur l'utilisation du chiffrement côté serveur Amazon S3 pour chiffrer vos données, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).
7. Si vous avez choisi le chiffrement côté serveur avec AWS Key Management Service clés (SSE-KMS) ou le chiffrement côté serveur double couche avec AWS Key Management Service clés (DSSE-KMS), procédez comme suit :

a. Sous CléAWS KMS , spécifiez votre clé KMS de l'une des manières suivantes :

- Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans la liste des clés disponibles.

  La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez la section Clés et AWS clés client dans le Guide du AWS Key Management Service développeur.

- Pour saisir l'ARN de la clé KMS, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de votre clé KMS dans le champ qui s'affiche.

- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

  Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS activées au même endroit Région AWS que le bucket. Lorsque vous choisissez Choisissez une clé parmi vos clés KMS, la console S3 ne répertorie que 100 clés KMS par Région. Si vous avez plus de 100 clés KMS dans la même Région, vous ne pourrez voir que les 100 premières clés KMS dans la console S3. Pour utiliser une clé KMS qui ne figure pas dans la console, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de la clé KMS.
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 prend uniquement en charge que les clés KMS de chiffrement symétriques. Pour plus d'informations sur ces clés, consultez Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur l'utilisation de SSE-KMS avec Amazon S3, consultez Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS). Pour en savoir plus sur

l'utilisation de DSSE-KMS, consultez the section called "Chiffrement double couche côté serveur (DSSE-KMS)".

b. Lorsque vous configurez votre compartiment pour utiliser le chiffrement par défaut avec SSE-KMS, vous pouvez également activer la clé de compartiment S3. Les clés de compartiment S3 réduisent le coût du chiffrement en diminuant le trafic de demandes d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

   Pour utiliser les clés de compartiment S3, sous la Clé de compartiment, choisissez Activer.

> **Note**
>
> Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS.

8. Sélectionnez Enregistrer les modifications.

À l'aide du AWS CLI

Ces exemples montrent comment configurer le chiffrement par défaut en utilisant SSE-S3 ou SSE-KMS avec une clé de compartiment S3.

Pour plus d'informations sur le chiffrement par défaut, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Pour plus d'informations sur l'utilisation du AWS CLI pour configurer le chiffrement par défaut, consultez put-bucket-encryption.

Example — Chiffrement par défaut avec SSE-S3

Cet exemple montre comment configurer le chiffrement du compartiment par défaut avec les clés gérées par Amazon S3.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
        {
            "ApplyServerSideEncryptionByDefault": {
                "SSEAlgorithm": "AES256"
            }
        }
    ]
}'
```

Example — Chiffrement par défaut avec SSE-KMS à l'aide d'une clé de compartiment S3

Cet exemple configure le chiffrement du compartiment par défaut avec SSE-KMS à l'aide d'une clé de compartiment S3.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
    "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

Utilisation de l'API REST

Utilisez l'opération `PutBucketEncryption` de l'API REST pour activer le chiffrement par défaut et définir le type de chiffrement côté serveur à utiliser : SSE-S3, SSE-KMS ou DSSE-KMS.

Pour plus d'informations, consultez PutBucketEncryption dans la Référence d'API Amazon Simple Storage Service.

Surveillance du chiffrement par défaut avec Amazon AWS CloudTrail et Amazon EventBridge

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Vous pouvez suivre les demandes de configuration de chiffrement par défaut pour les compartiments Amazon S3 à l'aide d'événements AWS CloudTrail . Les noms d'événements d'API suivants sont utilisés dans CloudTrail les journaux :

- `PutBucketEncryption`
- `GetBucketEncryption`
- `DeleteBucketEncryption`

Vous pouvez également créer des EventBridge règles correspondant aux CloudTrail événements de ces appels d'API. Pour plus d'informations sur CloudTrail les événements, consultezActiver la journalisation des objets d'un compartiment à l'aide de la console. Pour plus d'informations sur les EventBridge événements, consultez la section Événements de Services AWS.

Vous pouvez utiliser CloudTrail les journaux pour les actions Amazon S3 au niveau de l'objet à suivre `PUT` et pour les `POST` demandes adressées à Amazon S3. Vous pouvez utiliser ces actions pour vérifier si le chiffrement par défaut est utilisé pour chiffrer des objets lorsque les demandes `PUT` entrantes n'ont pas d'en-têtes de chiffrement.

Quand Amazon S3 chiffre un objet selon les paramètres de chiffrement par défaut, le journal inclut l'un des champs suivants comme paire nom-valeur : `"SSEApplied":"Default_SSE_S3"`, `"SSEApplied":"Default_SSE_KMS"` ou `"SSEApplied":"Defa`

Quand Amazon S3 chiffre un objet en utilisant les en-têtes de chiffrement `PUT`, le journal inclut l'un des champs suivants comme paire nom-valeur : `"SSEApplied":"SSE_S3"`, `"SSEApplied":"SSE_KMS"`, `"SSEApplied":"DSSE_KMS"` ou `"SSEApplied":"SSE_C"`.

Pour les chargements en plusieurs parties, cette information est incluse dans vos demandes d'opération d'API `InitiateMultipartUpload`. Pour plus d'informations sur l'utilisation CloudTrail de et CloudWatch, consultezJournalisation et surveillance dans Amazon S3.

FAQ sur le chiffrement par défaut

Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. SSE-S3, qui utilise la norme de chiffrement avancé 256 bits (AES-256), est automatiquement appliqué à tous les nouveaux compartiments et à tout compartiment S3 existant qui n'a pas déjà un chiffrement par défaut

configuré. L'état de chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour les téléchargements de nouveaux objets est disponible dans les AWS CloudTrail journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface (AWS CLI) et le AWS SDKs.

Les sections suivantes répondent aux questions concernant cette mise à jour.

Amazon S3 modifie-t-il les paramètres de chiffrement par défaut de mes compartiments existants pour lesquels le chiffrement par défaut est déjà configuré ?

Non Aucune modification n'est apportée à la configuration de chiffrement par défaut pour un compartiment existant sur lequel le chiffrement SSE-S3 ou le chiffrement côté serveur avec AWS Key Management Service (AWS KMS) clés (SSE-KMS) sont déjà configurés. Pour plus d'informations sur la manière de définir le comportement de chiffrement par défaut pour les compartiments, consultez Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3. Pour plus d'informations sur les paramètres de chiffrement de SSE-S3 et SSE-KMS, consultez Protection des données avec le chiffrement côté serveur.

Le chiffrement par défaut est-il activé sur mes compartiments existants qui n'ont pas de chiffrement par défaut configuré ?

Oui. Amazon S3 configure désormais le chiffrement par défaut de tous les compartiments non chiffrés existants pour appliquer le chiffrement côté serveur avec les clés gérées S3 (SSE-S3) comme niveau de base du chiffrement pour les nouveaux objets chargés dans ces compartiments. Les objets qui se trouvent déjà dans un compartiment non chiffré existant ne seront pas automatiquement chiffrés.

Comment puis-je afficher l'état de chiffrement par défaut des nouveaux chargements d'objets ?

À l'heure actuelle, vous pouvez consulter l'état de chiffrement par défaut des nouveaux objets chargés dans les AWS CloudTrail journaux, S3 Inventory et S3 Storage Lens, sur la console Amazon S3, et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface (AWS CLI) et le AWS SDKs.

- Pour consulter vos CloudTrail événements, reportez-vous à la section Affichage CloudTrail des événements dans la CloudTrail console du Guide de AWS CloudTrail l'utilisateur. CloudTrail les journaux fournissent le suivi des API `PUT` et des `POST` requêtes adressées à Amazon S3. Lorsque le chiffrement par défaut est utilisé pour chiffrer des objets dans vos compartiments, les CloudTrail journaux `PUT` et les demandes d'`POST`API incluront le champ suivant comme paire nom-valeur :. `"SSEApplied":"Default_SSE_S3"`

- Pour afficher l'état de chiffrement automatique des nouveaux objets chargés dans S3 Inventory, configurez un rapport S3 Inventory pour inclure le champ de métadonnées Encryption (Chiffrement), puis consultez l'état de chiffrement de chaque nouvel objet dans le rapport. Pour plus d'informations, consultez Configuration d'Amazon S3 Inventory.
- Pour consulter l'état de chiffrement automatique des nouveaux chargements d'objets dans S3 Storage Lens, configurez un tableau de bord S3 Storage Lens et consultez les mesures relatives à Octets chiffrés et Nombre d'objets chiffrés dans la catégorie Protection des données du tableau de bord. Pour plus d'informations, consultez Utilisation de la console S3 et Afficher les métriques S3 Storage Lens sur les tableaux de bord.
- Pour afficher le statut du chiffrement automatique au niveau du compartiment dans la console Amazon S3, vérifiez le chiffrement par défaut de vos compartiments Amazon S3 dans la console Amazon S3. Pour de plus amples informations, veuillez consulter Configuration du chiffrement par défaut.
- Pour afficher l'état du chiffrement automatique sous la forme d'un en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface (AWS CLI) et le AWS SDKs, vérifiez l'en-tête de réponse `x-amz-server-side-encryption` lorsque vous utilisez une action d'objet APIs, telle que PutObjectet GetObject.

Que dois-je faire pour profiter de ce changement ?

Vous n'êtes pas tenu d'apporter des modifications à vos applications existantes. Le chiffrement par défaut étant activé pour tous vos compartiments, tous les nouveaux objets chargés sur Amazon S3 sont automatiquement chiffrés.

Puis-je désactiver le chiffrement des nouveaux objets qui sont enregistrés dans mon compartiment ?

Non. SSE-S3 est le nouveau niveau de base du chiffrement qui est appliqué à tous les nouveaux objets chargés dans votre compartiment. Vous ne pouvez plus désactiver le chiffrement pour les nouveaux chargements d'objets.

Y aura-t-il une incidence sur mes frais ?

Non. Le chiffrement par défaut avec SSE-S3 est disponible sans coût supplémentaire. Vous serez facturé pour le stockage, les requêtes et les autres fonctionnalités de S3, comme d'habitude. Pour en savoir plus sur la tarification, consultez Tarification Amazon S3.

Amazon S3 va-t-il chiffrer mes objets existants qui ne sont pas chiffrés ?

Non. À partir du 5 janvier 2023, Amazon S3 ne chiffrera automatiquement que les nouveaux chargements d'objets. Pour chiffrer des objets existants, vous pouvez utiliser les opérations par lots S3 pour créer des copies chiffrées de vos objets. Ces copies chiffrées conserveront les données et le nom de l'objet existant et seront chiffrées à l'aide des clés de chiffrement que vous spécifiez. Pour plus de détails, consultez Encrypting objects with Amazon S3 Batch Operations (Chiffrement d'objets avec les opérations par lot Amazon S3) dans le blog sur le stockage AWS .

Je n'ai pas activé le chiffrement pour mes compartiments avant cette version. Dois-je modifier la façon dont j'accède aux objets ?

Non. Le chiffrement par défaut avec SSE-S3 chiffre automatiquement vos données lorsqu'elles sont enregistrées sur Amazon S3 et les déchiffre pour vous lorsque vous y accédez. Il n'y a aucun changement dans la façon dont vous accédez aux objets qui sont automatiquement chiffrés.

Dois-je modifier la façon dont j'accède à mes objets chiffrés côté client ?

Non. Tous les objets chiffrés côté client qui sont chiffrés avant d'être chargés dans Amazon S3 arrivent sous forme d'objets texte chiffré dans Amazon S3. Ces objets seront désormais dotés d'une couche supplémentaire de chiffrement SSE-S3. Vos charges de travail qui utilisent des objets chiffrés côté client ne nécessiteront aucune modification de vos services clients ou de vos paramètres d'autorisation.

> **Note**
>
> HashiCorp Les utilisateurs de Terraform qui n'utilisent pas de version mise à jour du AWS fournisseur peuvent constater une dérive inattendue après avoir créé de nouveaux compartiments S3 sans configuration de chiffrement définie par le client. Pour éviter cette dérive, mettez à jour la version de votre AWS fournisseur Terraform vers l'une des versions suivantes : n'importe quelle 4.x version3.76.1, ou. 2.70.4

Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur

les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Tous les nouveaux chargements d'objets dans les compartiments Amazon S3 sont chiffrés par défaut à l'aide du chiffrement côté serveur avec les clés gérées Amazon S3 (SSE-S3).

Le chiffrement côté serveur protège les données au repos. Amazon S3 chiffre chaque objet à l'aide d'une clé unique. Comme protection supplémentaire, il chiffre la clé elle-même à l'aide d'une clé dont il effectue une rotation régulière. Le chiffrement côté serveur Amazon S3 utilise le mode AES-GCM (Advanced Encryption Standard Galois/Counter Mode) 256 bits pour chiffrer tous les objets chargés.

L'utilisation du chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) n'entraîne pas de frais supplémentaires. Toutefois, les demandes de configuration de la fonction de chiffrement par défaut seront facturées comme des demandes Amazon S3 standard. Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3.

Si vous souhaitez que vos chargements de données soient chiffrés à l'aide de clés gérées uniquement par Amazon S3, vous pouvez utiliser la politique de compartiment suivante. Par exemple, la politique de compartiment suivante refuse les autorisations de charger un objet si la demande n'inclut pas l'en-tête `x-amz-server-side-encryption` demandant le chiffrement côté serveur :

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PutObjectPolicy",
  "Statement": [
    {
      "Sid": "DenyObjectsThatAreNotSSES3",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
      "Condition": {
```

```
        "StringNotEquals": {
          "s3:x-amz-server-side-encryption": "AES256"
        }
      }
    }
   ]
}
```

> **Note**
>
> Un chiffrement côté serveur chiffre uniquement les données d'objet, pas les métadonnées d'objet.

Prise en charge de l'API pour le chiffrement côté serveur

Le chiffrement est configuré par défaut pour tous les compartiments Amazon S3, et tous les nouveaux objets qui sont chargés dans un compartiment S3 sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment dans Amazon S3. Pour utiliser un autre type de chiffrement, vous pouvez soit spécifier le type de chiffrement côté serveur à utiliser dans vos PUT demandes S3, soit mettre à jour la configuration de chiffrement par défaut dans le compartiment de destination.

Si vous souhaitez spécifier un type de chiffrement différent dans vos PUT demandes, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), le chiffrement double couche côté serveur avec des clés (DSSE-KMS) ou le chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C). Si vous souhaitez définir une autre configuration de chiffrement par défaut dans le compartiment de destination, vous pouvez utiliser SSE-KMS ou DSSE-KMS.

Pour plus d'informations sur la modification de la configuration de chiffrement par défaut pour vos compartiments à usage général, consultezConfiguration du chiffrement par défaut.

Lorsque vous modifiez la configuration de chiffrement par défaut de votre compartiment en SSE-KMS, le type de chiffrement des objets Amazon S3 existants dans le compartiment n'est pas modifié. Pour modifier le type de chiffrement de vos objets préexistants après avoir mis à jour la configuration de chiffrement par défaut vers SSE-KMS, vous pouvez utiliser Amazon S3 Batch Operations. Vous fournissez à S3 Batch Operations une liste d'objets, et Batch Operations appelle l'opération d'API

correspondante. Vous pouvez utiliser cette Copie d'objets action pour copier des objets existants, ce qui les réécrit dans le même compartiment que les objets chiffrés SSE-KMS. Une tâche d'opérations par lots peut effectuer l'opération spécifiée sur des milliards d'objets. Pour plus d'informations, consultez Exécution d'opérations groupées sur des objets avec les opérations par lot le billet de blog sur le AWS stockage Comment chiffrer rétroactivement des objets existants dans Amazon S3 à l'aide de S3 Inventory, Amazon Athena et S3 Batch Operations.

Pour configurer le chiffrement côté serveur à l'aide du REST de création d'objets APIs, vous devez fournir l'en-tête de `x-amz-server-side-encryption` demande. Pour plus d'informations sur le REST APIs, consultezUtilisation de l'API REST.

Les Amazon S3 suivants APIs prennent en charge cet en-tête :

- Opérations PUT : spécifiez l'en-tête de demande lors du chargement des données grâce à l'API PUT. Pour plus d'informations, consultez Objet PUT.
- Lancement du chargement partitionné : spécifiez l'en-tête dans la demande initiale lors du chargement d'objets volumineux grâce à l'API de chargement partitionné. Pour plus d'informations, consultez Lancement du chargement partitionné.
- Opérations COPY : lorsque vous copiez un objet, vous disposez à la fois d'un objet source et d'un objet cible. Pour plus d'informations, consultez Objet PUT - Copy.

> **Note**
>
> Lors de l'utilisation d'une opération `POST` pour charger un objet, à la place de l'en-tête de demande, vous fournissez les mêmes informations dans les champs du formulaire. Pour plus d'informations, consultez POST Object.

Ils fournissent AWS SDKs également un wrapper APIs que vous pouvez utiliser pour demander un chiffrement côté serveur. Vous pouvez également utiliser le AWS Management Console pour télécharger des objets et demander un chiffrement côté serveur.

Pour obtenir des informations plus générales, consultez Concepts AWS KMS dans le Guide du développeur AWS Key Management Service .

Rubriques

- Spécification du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

Spécification du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)

Le chiffrement est configuré par défaut pour tous les compartiments Amazon S3, et tous les nouveaux objets qui sont chargés dans un compartiment S3 sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment dans Amazon S3. Pour utiliser un autre type de chiffrement, vous pouvez soit spécifier le type de chiffrement côté serveur à utiliser dans vos PUT demandes S3, soit mettre à jour la configuration de chiffrement par défaut dans le compartiment de destination.

Si vous souhaitez spécifier un type de chiffrement différent dans vos PUT demandes, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), le chiffrement double couche côté serveur avec des clés (DSSE-KMS) ou le chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C). Si vous souhaitez définir une autre configuration de chiffrement par défaut dans le compartiment de destination, vous pouvez utiliser SSE-KMS ou DSSE-KMS.

Pour plus d'informations sur la modification de la configuration de chiffrement par défaut pour vos compartiments à usage général, consultezConfiguration du chiffrement par défaut.

Lorsque vous modifiez la configuration de chiffrement par défaut de votre compartiment en SSE-KMS, le type de chiffrement des objets Amazon S3 existants dans le compartiment n'est pas modifié. Pour modifier le type de chiffrement de vos objets préexistants après avoir mis à jour la configuration de chiffrement par défaut vers SSE-KMS, vous pouvez utiliser Amazon S3 Batch Operations. Vous fournissez à S3 Batch Operations une liste d'objets, et Batch Operations appelle l'opération d'API correspondante. Vous pouvez utiliser cette Copie d'objets action pour copier des objets existants, ce qui les réécrit dans le même compartiment que les objets chiffrés SSE-KMS. Une tâche d'opérations par lots peut effectuer l'opération spécifiée sur des milliards d'objets. Pour plus d'informations, consultez Exécution d'opérations groupées sur des objets avec les opérations par lot le billet de blog sur le AWS stockage Comment chiffrer rétroactivement des objets existants dans Amazon S3 à l'aide de S3 Inventory, Amazon Athena et S3 Batch Operations.

Vous pouvez spécifier SSE-S3 à l'aide de la console S3 APIs AWS SDKs, REST et AWS Command Line Interface ()AWS CLI. Pour de plus amples informations, veuillez consulter Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.

Utilisation de la console S3

Cette rubrique décrit comment définir ou modifier le type de chiffrement qu'un objet utilise à l'aide de la AWS Management Console. Lorsque vous copiez un objet en utilisant la console, Amazon S3

copie l'objet en l'état. Cela signifie que si l'objet source est chiffré, l'objet cible est également chiffré. La console vous permet d'ajouter ou de modifier le chiffrement d'un objet.

> **Note**
>
> - Vous pouvez modifier le chiffrement d'un objet si sa taille est inférieure à 5 Go. Si la taille de votre objet est supérieure à 5 Go, vous devez utiliser le AWS CLIou AWS SDKspour modifier le chiffrement d'un objet.
> - Pour obtenir la liste des autorisations supplémentaires requises pour modifier le chiffrement d'un objet, consultez the section called "Autorisations requises pour les opérations d'API S3". Pour obtenir un exemple de politiques qui accorde ces autorisations, consultez the section called "Exemples de politiques basées sur l'identité".
> - Si vous modifiez le chiffrement d'un objet, un nouvel objet est créé pour remplacer l'ancien. Si la gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

Pour modifier le chiffrement d'un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments, puis l'onglet Compartiments à usage général. Accédez au compartiment ou au dossier Amazon S3 contenant les objets que vous souhaitez modifier.
3. Cochez la case correspondant aux objets à modifier.
4. Dans le menu Actions, choisissez Modifier le chiffrement côté serveur dans la liste d'options qui s'affiche.
5. Accédez à la section Chiffrement côté serveur.
6. Sous Paramètres de chiffrement, choisissez Utiliser les paramètres du compartiment pour le chiffrement par défaut ou Ignorer les paramètres du compartiment pour le chiffrement par défaut.
7. Si vous avez choisi Ignorer les paramètres de chiffrement par défaut du compartiment, configurez les paramètres de chiffrement suivants.

    - Sous Type de chiffrement, choisissez Server-side encryption with Amazon S3 managed keys (SSE-S3) (Chiffrement côté serveur avec clés de chiffrement gérées par Amazon S3

(SSE-S3)). SSE-S3 utilise l'un des chiffrements par bloc les plus puissants qui existent, Advanced Encryption Standard à 256 bits (AES-256) pour chiffrer chaque objet. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

8. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.
9. Sélectionnez Save Changes (Enregistrer les modifications).

> **Note**
>
> Cette action applique le chiffrement à tous les objets spécifiés. Lorsque vous chiffrez des dossiers, attendez la fin de l'opération d'enregistrement pour ajouter de nouveaux objets au dossier.

Utilisation de l'API REST

Lors de la création d'un objet (c'est-à-dire lorsque vous chargez un nouvel objet ou effectuez une copie d'un objet existant), vous pouvez spécifier si vous souhaitez qu'Amazon S3 chiffre vos données avec des clés gérées par Amazon S3 (SSE-S3) en ajoutant l'en-tête `x-amz-server-side-encryption` à la demande. Définissez la valeur de l'en-tête sur l'algorithme de chiffrement `AES256` pris en charge par Amazon S3. Amazon S3 confirme que votre objet est stocké avec SSE-KMS en renvoyant l'en-tête de réponse `x-amz-server-side-encryption`.

Les opérations d'API de chargement REST suivantes acceptent l'en-tête de demande `x-amz-server-side-encryption`.

- PUT Object
- PUT Object - Copy
- POST Object
- Lancement du chargement partitionné

Lors du chargement d'objets volumineux à l'aide de l'opération d'API de chargement partitionné, vous pouvez spécifier un chiffrement côté serveur en ajoutant l'en-tête `x-amz-server-side-encryption` à la demande de lancement de chargement partitionné. Lorsque vous copiez un objet existant, que l'objet source soit chiffré ou non, l'objet de destination n'est pas chiffré sauf si vous demandez explicitement un chiffrement côté serveur.

Les en-têtes de réponse des opérations d'API REST suivantes renvoient l'en-tête `x-amz-server-side-encryption` lorsqu'un objet est stocké grâce à SSE-S3.

- PUT Object
- PUT Object - Copy
- POST Object
- Lancement du chargement partitionné
- Chargement d'une partie
- Chargement d'une partie (Copy)
- Achèvement du chargement partitionné
- Get Object
- Head Object

> **Note**
>
> N'envoyez pas d'en-têtes de demande de chiffrement pour les demandes `GET` et `HEAD` si votre objet utilise SSE-S3 ou vous obtiendrez une erreur code d'état HTTP 400 (Demande erronée).

À l'aide du AWS SDKs

Lors de l'utilisation AWS SDKs, vous pouvez demander à Amazon S3 d'utiliser le chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3). Cette section fournit des exemples d'utilisation du AWS SDKs dans plusieurs langues. Pour plus d'informations sur les autres SDKs, reportez-vous à la section Exemples de code et bibliothèques.

Java

Lorsque vous utilisez le AWS SDK pour Java pour télécharger un objet, vous pouvez utiliser SSE-S3 pour le chiffrer. Pour demander un chiffrement côté serveur, utilisez la propriété

`ObjectMetadata` de la demande `PutObjectRequest` pour définir l'en-tête de demande `x-amz-server-side-encryption`. Lorsque vous appelez la méthode `putObject()` du `AmazonS3Client`, Amazon S3 chiffre et enregistre les données.

Vous pouvez également demander le chiffrement SSE-S3 lors du chargement d'objet avec l'opération d'API de chargement partitionné :

- Lorsque vous utilisez l'opération d'API de chargement partitionné de haut niveau, vous utilisez les méthodes `TransferManager` pour appliquer le chiffrement côté serveur aux objets à mesure que vous les chargez. Vous pouvez utiliser n'importe quelle méthode de chargement qui accepte `ObjectMetadata` comme paramètre. Pour plus d'informations, consultez Chargement d'un objet à l'aide du chargement partitionné.
- Lorsque vous utilisez l'opération d'API de chargement partitionné de bas niveau, vous spécifiez le chiffrement côté serveur quand vous lancez le chargement partitionné. Vous ajoutez la propriété `ObjectMetadata` en appelant la méthode `InitiateMultipartUploadRequest.setObjectMetadata()`. Pour plus d'informations, consultez Utilisation de AWS SDKs (API de bas niveau).

Vous ne pouvez pas modifier directement l'état de chiffrement d'un objet (chiffrer un objet non chiffré ou déchiffrer un objet chiffré). Pour modifier l'état de chiffrement d'un objet, vous effectuez une copie de l'objet, en spécifiant l'état de chiffrement voulu pour la copie, puis supprimez l'objet d'origine. Amazon S3 chiffre l'objet copié uniquement si vous demandez explicitement un chiffrement côté serveur. Pour demander le chiffrement de l'objet copié via l'API Java, utilisez la propriété `ObjectMetadata` pour spécifier le chiffrement côté serveur dans la demande `CopyObjectRequest`.

Example exemple

L'exemple suivant illustre comment définir le chiffrement côté serveur à l'aide du kit AWS SDK pour Java. Il explique comment effectuer les tâches suivantes :

- Chargez un nouvel objet à l'aide de SSE-S3.
- Modifier l'état de chiffrement d'un objet (dans cet exemple, chiffrer un objet précédemment non chiffré) en effectuant une copie de l'objet.
- Vérifier l'état de chiffrement de l'objet.

Pour plus d'informations sur le chiffrement côté serveur, consultez Utilisation de l'API REST. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.internal.SSEResultBase;
import com.amazonaws.services.s3.model.*;

import java.io.ByteArrayInputStream;

public class SpecifyServerSideEncryption {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyNameToEncrypt = "*** Key name for an object to upload and encrypt
 ***";
        String keyNameToCopyAndEncrypt = "*** Key name for an unencrypted object to
 be encrypted by copying ***";
        String copiedObjectKeyName = "*** Key name for the encrypted copy of the
 unencrypted object ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();

            // Upload an object and encrypt it with SSE.
            uploadObjectWithSSEEncryption(s3Client, bucketName, keyNameToEncrypt);

            // Upload a new unencrypted object, then change its encryption state
            // to encrypted by making a copy.
            changeSSEEncryptionStatusByCopying(s3Client,
                    bucketName,
                    keyNameToCopyAndEncrypt,
                    copiedObjectKeyName);
```

```
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void uploadObjectWithSSEEncryption(AmazonS3 s3Client, String
bucketName, String keyName) {
        String objectContent = "Test object encrypted with SSE";
        byte[] objectBytes = objectContent.getBytes();

        // Specify server-side encryption.
        ObjectMetadata objectMetadata = new ObjectMetadata();
        objectMetadata.setContentLength(objectBytes.length);

objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
        PutObjectRequest putRequest = new PutObjectRequest(bucketName,
                keyName,
                new ByteArrayInputStream(objectBytes),
                objectMetadata);

        // Upload the object and check its encryption status.
        PutObjectResult putResult = s3Client.putObject(putRequest);
        System.out.println("Object \"" + keyName + "\" uploaded with SSE.");
        printEncryptionStatus(putResult);
    }

    private static void changeSSEEncryptionStatusByCopying(AmazonS3 s3Client,
            String bucketName,
            String sourceKey,
            String destKey) {
        // Upload a new, unencrypted object.
        PutObjectResult putResult = s3Client.putObject(bucketName, sourceKey,
"Object example to encrypt by copying");
        System.out.println("Unencrypted object \"" + sourceKey + "\" uploaded.");
        printEncryptionStatus(putResult);

        // Make a copy of the object and use server-side encryption when storing the
        // copy.
```

```
        CopyObjectRequest request = new CopyObjectRequest(bucketName,
                sourceKey,
                bucketName,
                destKey);
        ObjectMetadata objectMetadata = new ObjectMetadata();

 objectMetadata.setSSEAlgorithm(ObjectMetadata.AES_256_SERVER_SIDE_ENCRYPTION);
        request.setNewObjectMetadata(objectMetadata);

        // Perform the copy operation and display the copy's encryption status.
        CopyObjectResult response = s3Client.copyObject(request);
        System.out.println("Object \"" + destKey + "\" uploaded with SSE.");
        printEncryptionStatus(response);

        // Delete the original, unencrypted object, leaving only the encrypted copy
 in
        // Amazon S3.
        s3Client.deleteObject(bucketName, sourceKey);
        System.out.println("Unencrypted object \"" + sourceKey + "\" deleted.");
    }

    private static void printEncryptionStatus(SSEResultBase response) {
        String encryptionStatus = response.getSSEAlgorithm();
        if (encryptionStatus == null) {
            encryptionStatus = "Not encrypted with SSE";
        }
        System.out.println("Object encryption status is: " + encryptionStatus);
    }
}
```

.NET

Lorsque vous chargez un objet, vous pouvez indiquer à Amazon S3 de le chiffrer. Pour modifier l'état de chiffrement d'un objet existant, vous effectuez une copie de l'objet et supprimez l'objet source. Par défaut, l'opération de copie ne chiffre la cible que si vous demandez explicitement un chiffrement côté serveur de l'objet cible. Pour spécifier SSE-S3 dans `CopyObjectRequest`, ajoutez ce qui suit :

```
ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
```

Pour obtenir un exemple pratique sur la façon de copier un objet, consultez À l'aide du AWS SDKs.

L'exemple suivant permet de charger un objet. Dans la demande, l'exemple indique à Amazon S3 de chiffrer l'objet. L'exemple récupère ensuite les métadonnées de l'objet et vérifie la méthode de chiffrement utilisée. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SpecifyServerSideEncryptionTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for object created ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            WritingAnObjectAsync().Wait();
        }

        static async Task WritingAnObjectAsync()
        {
            try
            {
                var putRequest = new PutObjectRequest
                {
                    BucketName = bucketName,
                    Key = keyName,
                    ContentBody = "sample text",
                    ServerSideEncryptionMethod = ServerSideEncryptionMethod.AES256
                };
```

```
                var putResponse = await client.PutObjectAsync(putRequest);

                // Determine the encryption state of an object.
                GetObjectMetadataRequest metadataRequest = new
 GetObjectMetadataRequest
                {
                    BucketName = bucketName,
                    Key = keyName
                };
                GetObjectMetadataResponse response = await
 client.GetObjectMetadataAsync(metadataRequest);
                ServerSideEncryptionMethod objectEncryption =
 response.ServerSideEncryptionMethod;

                Console.WriteLine("Encryption method used: {0}",
 objectEncryption.ToString());
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
 an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

Cette rubrique explique comment utiliser les classes de la version 3 de AWS SDK pour PHP pour ajouter SSE-S3 aux objets que vous chargez sur Amazon S3. Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

Pour charger un objet dans Amazon S3, utilisez la méthode Aws\S3\S3Client::putObject(). Pour ajouter l'en-tête de demande `x-amz-server-side-encryption` à votre demande de chargement, spécifiez le paramètre `ServerSideEncryption` avec la valeur `AES256` comme illustré dans l'exemple de code suivant. Pour plus d'informations sur les demandes de chiffrement côté serveur, consultez Utilisation de l'API REST.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

// $filepath should be an absolute path to a file on disk.
$filepath = '*** Your File Path ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Upload a file with server-side encryption.
$result = $s3->putObject([
    'Bucket'               => $bucket,
    'Key'                  => $keyname,
    'SourceFile'           => $filepath,
    'ServerSideEncryption' => 'AES256',
]);
```

En réponse, Amazon S3 renvoie l'en-tête `x-amz-server-side-encryption` avec la valeur de l'algorithme de chiffrement qui a été utilisé pour chiffrer les données de l'objet.

Lorsque vous chargez des objets volumineux à l'aide de l'opération d'API de chargement partitionné, vous pouvez spécifier SSE-S3 pour les objets que vous chargez, comme suit :

- Lorsque vous utilisez l'opération d'API de téléchargement partitionné de bas niveau, spécifiez le chiffrement côté serveur lorsque vous appelez la méthode Aws \ S3 \ S3Client : : (). createMultipartUpload Pour ajouter l'en-tête `x-amz-server-side-encryption` à la demande, spécifiez le paramètre `array` avec la clé `ServerSideEncryption` en lui donnant la valeur `AES256`. Pour plus d'informations sur l'opération d'API de chargement partitionné de bas niveau, consultez Utilisation de AWS SDKs (API de bas niveau).
- Lorsque vous utilisez l'opération d'API de téléchargement partitionné de haut niveau, spécifiez le chiffrement côté serveur à l'aide du `ServerSideEncryption` paramètre de l'CreateMultipartUploadopération d'API. Pour obtenir un exemple d'utilisation de la méthode

`setOption()` avec l'opération d'API de chargement partitionné de haut niveau, consultez Chargement d'un objet à l'aide du chargement partitionné.

Pour déterminer l'état de chiffrement d'un objet existant, récupérez les métadonnées d'objet en appelant la méthode Aws\S3\S3Client::headObject() comme illustré dans l'exemple de code PHP suivant.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$bucket = '*** Your Bucket Name ***';
$keyname = '*** Your Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Check which server-side encryption algorithm is used.
$result = $s3->headObject([
    'Bucket' => $bucket,
    'Key'    => $keyname,
]);
echo $result['ServerSideEncryption'];
```

Pour changer l'état de chiffrement d'un objet existant, faites une copie de l'objet grâce à la méthode Aws\S3\S3Client::copyObject() et supprimez l'objet source. Par défaut, `copyObject()` ne chiffre pas la cible, sauf si vous demandez explicitement un chiffrement côté serveur de l'objet de destination à l'aide du paramètre `ServerSideEncryption` avec la valeur `AES256`. L'exemple de code PHP suivant fait une copie d'un objet et ajoute un chiffrement côté serveur à l'objet copié.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;

$sourceBucket = '*** Your Source Bucket Name ***';
$sourceKeyname = '*** Your Source Object Key ***';
```

```
$targetBucket = '*** Your Target Bucket Name ***';
$targetKeyname = '*** Your Target Object Key ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);

// Copy an object and add server-side encryption.
$s3->copyObject([
    'Bucket'               => $targetBucket,
    'Key'                  => $targetKeyname,
    'CopySource'           => "$sourceBucket/$sourceKeyname",
    'ServerSideEncryption' => 'AES256',
]);
```

Pour plus d'informations, consultez les rubriques suivantes :

- AWS SDK pour PHP pour la classe Amazon S3 Aws \ S3 \ S3Client
- Documentation AWS SDK pour PHP

Ruby

Lorsque vous utilisez le AWS SDK pour Ruby pour télécharger un objet, vous pouvez spécifier que l'objet doit être stocké chiffré au repos avec SSE-S3. Lorsque vous relisez l'objet, il est automatiquement déchiffré.

L'exemple de AWS SDK pour Ruby version 3 suivant montre comment spécifier qu'un fichier chargé sur Amazon S3 soit chiffré au repos.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectPutSseWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end
```

```
  def put_object_encrypted(object_content, encryption)
    @object.put(body: object_content, server_side_encryption: encryption)
    true
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't put your content to #{object.key}. Here's why: #{e.message}"
    false
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-encrypted-content"
  object_content = "This is my super-secret content."
  encryption = "AES256"

  wrapper = ObjectPutSseWrapper.new(Aws::S3::Object.new(bucket_name,
 object_content))
  return unless wrapper.put_object_encrypted(object_content, encryption)

  puts "Put your content into #{bucket_name}:#{object_key} and encrypted it with
 #{encryption}."
end

run_demo if $PROGRAM_NAME == __FILE__
```

L'exemple de code suivant montre comment déterminer l'état de chiffrement d'un objet existant.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectGetEncryptionWrapper
  attr_reader :object

  # @param object [Aws::S3::Object] An existing Amazon S3 object.
  def initialize(object)
    @object = object
  end

  # Gets the object into memory.
  #
  # @return [Aws::S3::Types::GetObjectOutput, nil] The retrieved object data if
 successful; otherwise nil.
```

```
  def object
    @object.get
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't get object #{@object.key}. Here's why: #{e.message}"
  end
end

# Example usage:
def run_demo
  bucket_name = "amzn-s3-demo-bucket"
  object_key = "my-object.txt"

  wrapper = ObjectGetEncryptionWrapper.new(Aws::S3::Object.new(bucket_name,
 object_key))
  obj_data = wrapper.get_object
  return unless obj_data

  encryption = obj_data.server_side_encryption.nil? ? 'no' :
 obj_data.server_side_encryption
  puts "Object #{object_key} uses #{encryption} encryption."
end

run_demo if $PROGRAM_NAME == __FILE__
```

Si un chiffrement côté serveur n'est pas utilisé pour l'objet stocké dans Amazon S3, la méthode renvoie `null`.

Pour modifier l'état de chiffrement d'un objet existant, effectuez une copie de l'objet et supprimez l'objet source. Par défaut, les méthodes de copie ne chiffrent la cible que si vous demandez explicitement un chiffrement côté serveur. Vous pouvez demander le chiffrement de l'objet cible en spécifiant la valeur `server_side_encryption` dans l'argument de hachage d'options, comme illustré dans l'exemple de code Ruby suivant. L'exemple de code montre comment copier un objet et chiffrer la copie avec SSE-S3.

```
require 'aws-sdk-s3'

# Wraps Amazon S3 object actions.
class ObjectCopyEncryptWrapper
  attr_reader :source_object

  # @param source_object [Aws::S3::Object] An existing Amazon S3 object. This is
 used as the source object for
```

```
  #                                          copy actions.
  def initialize(source_object)
    @source_object = source_object
  end

  # Copy the source object to the specified target bucket, rename it with the target
 key, and encrypt it.
  #
  # @param target_bucket [Aws::S3::Bucket] An existing Amazon S3 bucket where the
 object is copied.
  # @param target_object_key [String] The key to give the copy of the object.
  # @return [Aws::S3::Object, nil] The copied object when successful; otherwise,
 nil.
  def copy_object(target_bucket, target_object_key, encryption)
    @source_object.copy_to(bucket: target_bucket.name, key: target_object_key,
 server_side_encryption: encryption)
    target_bucket.object(target_object_key)
  rescue Aws::Errors::ServiceError => e
    puts "Couldn't copy #{@source_object.key} to #{target_object_key}. Here's why:
 #{e.message}"
  end
end

# Example usage:
def run_demo
  source_bucket_name = "amzn-s3-demo-bucket1"
  source_key = "my-source-file.txt"
  target_bucket_name = "amzn-s3-demo-bucket2"
  target_key = "my-target-file.txt"
  target_encryption = "AES256"

  source_bucket = Aws::S3::Bucket.new(source_bucket_name)
  wrapper = ObjectCopyEncryptWrapper.new(source_bucket.object(source_key))
  target_bucket = Aws::S3::Bucket.new(target_bucket_name)
  target_object = wrapper.copy_object(target_bucket, target_key, target_encryption)
  return unless target_object

  puts "Copied #{source_key} from #{source_bucket_name} to
 #{target_object.bucket_name}:#{target_object.key} and "\
       "encrypted the target with #{target_object.server_side_encryption}
 encryption."
end
```

```
run_demo if $PROGRAM_NAME == __FILE__
```

À l'aide du AWS CLI

Pour spécifier SSE-S3 lorsque vous chargez un objet à l'aide du AWS CLI, utilisez l'exemple suivant.

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key object-key-name --server-side-encryption AES256  --body file path
```

Pour plus d'informations, consultez put-object dans la Référence de la AWS CLI . Pour spécifier SSE-S3 lorsque vous copiez un objet à l'aide du AWS CLI, voir copy-object.

En utilisant AWS CloudFormation

Pour des exemples de configuration du chiffrement à l'aide d'un exemple AWS CloudFormation, reportez-vous aux sections Création d'un compartiment avec chiffrement par défaut et Création d'un compartiment en utilisant le chiffrement AWS KMS côté serveur avec une clé de compartiment S3 dans la `AWS::S3::Bucket ServerSideEncryptionRule` rubrique du Guide de l'AWS CloudFormation utilisateur.

Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS)

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Le chiffrement côté serveur est le chiffrement des données à leur destination par l'application ou le service qui les reçoit.

Amazon S3 active automatiquement le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) pour les nouveaux chargements d'objets.

Sauf indication contraire, les compartiments utilisent SSE-S3 par défaut pour chiffrer les objets. Toutefois, vous pouvez choisir de configurer les buckets pour qu'ils utilisent plutôt le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). Pour de plus amples informations, veuillez consulter Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS).

AWS KMS est un service qui combine du matériel et des logiciels sécurisés et hautement disponibles pour fournir un système de gestion des clés adapté au cloud. Amazon S3 utilise le chiffrement côté serveur avec AWS KMS (SSE-KMS) pour chiffrer les données de vos objets S3. En outre, lorsque SSE-KMS est demandé pour l'objet, la somme de contrôle S3, qui fait partie des métadonnées de l'objet, est stockée sous forme chiffrée. Pour plus d'informations sur le total de contrôle, consultez Vérification de l'intégrité des objets dans Amazon S3.

Si vous utilisez des clés KMS, vous pouvez les utiliser AWS KMS via l'API AWS Management Consoleou l'AWS KMS API pour effectuer les opérations suivantes :

- Créez, visualisez, modifiez, surveillez, activez ou désactivez, faites tourner et planifiez la suppression des clés KMS de manière centralisée.
- Définir les politiques qui contrôlent comment et par qui les clés KMS peuvent être utilisées.
- Vérifiez l'utilisation des clés KMS pour une utilisation correcte. L'audit est pris en charge par l'AWS KMS API mais pas par la AWS KMS console ;

Les contrôles de sécurité intégrés AWS KMS peuvent vous aider à respecter les exigences de conformité liées au chiffrement. Vous pouvez utiliser ces clés KMS pour protéger les données dans les compartiments Simple Storage Service (Amazon S3). Lorsque vous utilisez le chiffrement SSE-KMS avec un compartiment S3, celui-ci AWS KMS keys doit se trouver dans la même région que le compartiment.

L'utilisation entraîne des frais supplémentaires AWS KMS keys. Pour plus d'informations, consultez Concepts AWS KMS key dans le Guide du développeur AWS Key Management Service et Tarification AWS KMS.

Pour savoir comment autoriser les utilisateurs IAM à accéder aux compartiments chiffrés par KMS, consultez la section Mon compartiment Amazon S3 est chiffré par défaut à l'aide d'une clé

personnalisée. AWS KMS Comment puis-je autoriser les utilisateurs à effectuer des téléchargements depuis et vers le bucket ? dans le AWS re:Post Knowledge Center.

Autorisations

Pour réussir à envoyer une `PutObject` demande de chiffrement d'un objet avec une AWS KMS clé à Amazon S3, vous devez `kms:GenerateDataKey` disposer d'autorisations sur la clé. Pour télécharger un objet chiffré avec un AWS KMS key, vous devez `kms:Decrypt` disposer d'autorisations pour la clé. Pour effectuer un téléchargement partitionné afin de chiffrer un objet avec un AWS KMS key, vous devez disposer des `kms:Decrypt` autorisations `kms:GenerateDataKey` et pour la clé.

> **Important**
>
> Examinez attentivement les autorisations accordées dans les politiques des clés KMS. Limitez toujours les autorisations de politique clé KMS gérées par le client uniquement aux principaux et AWS services IAM qui doivent accéder à l'action clé appropriée. AWS KMS Pour plus d'informations, consultez la section Politiques clés dans AWS KMS.

Rubriques

- AWS KMS keys
- Clés de compartiment Amazon S3
- Exigence du chiffrement côté serveur
- Contexte de chiffrement
- Envoi de demandes pour des objets AWS KMS chiffrés
- Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS)
- Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3

AWS KMS keys

Lorsque vous utilisez le chiffrement côté serveur avec AWS KMS (SSE-KMS), vous pouvez utiliser la cléAWS gérée par défaut ou vous pouvez spécifier une clé gérée par le client que vous avez déjà créée. AWS KMS prend en charge le chiffrement des enveloppes. S3 utilise les AWS KMS fonctionnalités de chiffrement des enveloppes pour mieux protéger vos données. Le chiffrement d'enveloppe consiste à chiffrer vos données en texte brut avec une clé de données, puis à chiffrer

cette clé de données avec une clé KMS. Pour plus d'informations sur le chiffrement d'enveloppe, consultez Chiffrement d'enveloppe dans le Guide du développeur AWS Key Management Service .

Si vous ne spécifiez pas de clé gérée par le client, Amazon S3 Clé gérée par AWS en crée automatiquement une lorsque vous Compte AWS ajoutez un objet chiffré avec SSE-KMS à un bucket pour la première fois. Par défaut, Amazon S3 utilise cette clé KMS pour SSE-KMS.

> **Note**
>
> Les objets chiffrés en utilisant SSE-KMS avec des Clés gérées par AWS ne peuvent pas être partagés entre comptes. Si vous devez partager des données SSE-KMS entre comptes, vous devez utiliser une clé gérée par le client provenant de. AWS KMS

Si vous souhaitez utiliser une clé gérée par le client pour SSE-KMS, créez une clé gérée par le client à chiffrement symétrique avant de configurer SSE-KMS. Ensuite, lorsque vous configurez SSE-KMS pour votre compartiment, vous pouvez spécifier la clé gérée par le client existante. Pour plus d'informations sur la clé de chiffrement symétrique, consultez Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

En créant une clé gérée par le client, vous disposez de plus de flexibilité et d'un contrôle accru. Par exemple, vous pouvez créer, faire tourner et désactiver les clés gérés par le client. Vous pouvez également définir des contrôles d'accès et auditer les clés gérées par le client que vous utilisez pour protéger vos données. Pour plus d'informations sur les clés gérées et AWS gérées par le client, consultez la section Clés et AWS clés client dans le guide du AWS Key Management Service développeur.

> **Note**
>
> Lorsque vous utilisez le chiffrement côté serveur avec une clé gérée par le client qui est stockée dans un magasin de clés externe, contrairement aux clés KMS standard, vous êtes responsable de la disponibilité et de la durabilité de votre matériel de clé. Pour plus d'informations sur les magasins de clés externes et sur la manière dont ils modifient le modèle de responsabilité partagée, consultez Magasins de clés externes dans le Guide du développeur AWS Key Management Service .

Utilisation du chiffrement SSE-KMS pour les opérations intercomptes

Tenez compte des éléments suivants lors de l'utilisation du chiffrement pour les opérations inter-comptes :

- Si aucun nom de ressource AWS KMS key Amazon (ARN) ou alias n'est fourni au moment de la demande ou via la configuration de chiffrement par défaut du bucket, le Clé gérée par AWS (`aws/s3`) est utilisé.
- Si vous téléchargez ou accédez à des objets S3 à l'aide de principes AWS Identity and Access Management (IAM) identiques Compte AWS à ceux de votre clé KMS, vous pouvez utiliser le Clé gérée par AWS (). `aws/s3`
- Utilisez une clé gérée par le client si vous souhaitez accorder un accès intercompte à vos objets S3. Vous pouvez configurer la politique d'une clé gérée par le client afin d'autoriser l'accès à partir d'un autre compte.
- Si vous spécifiez une clé KMS gérée par le client, nous recommandons d'utiliser un ARN de clé KMS complet. Si vous utilisez plutôt un alias de clé KMS, AWS KMS la clé est résolue dans le compte du demandeur. En raison de ce comportement, les données peuvent être chiffrées avec une clé KMS qui appartient au demandeur, et non au propriétaire du compartiment.
- Vous devez spécifier une clé pour laquelle vous (le demandeur) avez obtenu l'autorisation de `Encrypt`. Pour en savoir plus, consultez Permettre aux utilisateurs de clés d'utiliser une clé KMS pour les opérations de chiffrement dans le Guide de l'utilisateur AWS Key Management Service .

Pour plus d'informations sur les circonstances dans lesquelles utiliser des clés gérées par le client et des clés KMS AWS gérées, consultez Dois-je utiliser une clé gérée par le client Clé gérée par AWS ou une clé gérée par le client pour chiffrer mes objets dans Amazon S3 ?

Flux de travail de chiffrement SSE-KMS

Si vous choisissez de chiffrer vos données à l'aide d'une clé gérée par le client Clé gérée par AWS ou d'une clé gérée par le client, AWS KMS et qu'Amazon S3 exécute les actions de chiffrement d'enveloppe suivantes :

1. Simple Storage Service (Amazon S3) demande une clé de données en texte brut et une copie de la clé chiffrée sous la clé KMS spécifiée.
2. AWS KMS génère une clé de données, la chiffre sous la clé KMS et envoie à la fois la clé de données en texte brut et la clé de données chiffrée à Amazon S3.

3. Amazon S3 chiffre les données à l'aide de la clé de données et supprime la clé en texte brut de la mémoire dès que possible après utilisation.
4. Simple Storage Service (Amazon S3) stocke la clé de données chiffrée sous forme de métadonnées avec les données chiffrées.

Lorsque vous demandez que vos données soient déchiffrées, Amazon S3 AWS KMS effectue les actions suivantes :

1. Amazon S3 envoie la clé de données chiffrée à AWS KMS dans une `Decrypt` demande.
2. AWS KMS déchiffre la clé de données chiffrée à l'aide de la même clé KMS et renvoie la clé de données en texte brut à Amazon S3.
3. Amazon S3 déchiffre les données chiffrées, en utilisant la clé des données en texte brut, et supprime la clé des données en texte brut de la mémoire dès que possible.

> **Important**
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 ne prend en charge que les clés KMS à chiffrement symétrique. Pour plus d'informations sur ces clés, consultez Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

Audit du chiffrement SSE-KMS

Pour identifier les requêtes qui spécifient SSE-KMS, vous pouvez utiliser les métriques Toutes les demandes SSE-KMS et % de toutes les demandes SSE-KMS dans les métriques Amazon S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Vous pouvez également utiliser le nombre de compartiments avec le chiffrement SSE-KMS activé et le pourcentage de compartiments avec le chiffrement SSE-KMS activé pour déterminer le nombre de compartiments (SSE-KMS) pour le chiffrement des compartiments par défaut. Pour plus d'informations, consultez Évaluer l'activité et l'utilisation de votre stockage avec S3 Storage Lens. Pour obtenir la liste complète des métriques, consultez le Glossaire des métriques S3 Storage Lens.

Pour vérifier l'utilisation de vos AWS KMS clés pour vos données cryptées SSE-KMS, vous pouvez utiliser AWS CloudTrail des journaux. Vous pouvez obtenir un aperçu de vos opérations cryptographiques, telles que GenerateDataKeyet Decrypt. CloudTrail prend en charge de nombreuses valeurs d'attribut pour filtrer votre recherche, notamment le nom de l'événement, le nom d'utilisateur et la source de l'événement.

Clés de compartiment Amazon S3

Lorsque vous configurez le chiffrement côté serveur à l'aide de AWS KMS (SSE-KMS), vous pouvez configurer vos compartiments pour utiliser les clés de compartiment S3 pour SSE-KMS. L'utilisation d'une clé au niveau du compartiment pour SSE-KMS peut réduire les coûts de vos AWS KMS demandes jusqu'à 99 % en diminuant le trafic de demandes d'Amazon S3 vers. AWS KMS

Lorsque vous configurez un compartiment de sorte qu'il utilise des clés de compartiment S3 pour SSE-KMS sur de nouveaux objets, AWS KMS génère une clé de niveau compartiment qui est utilisée pour créer des clés de données uniques pour les objets dans le compartiment. Cette clé de compartiment S3 est utilisée pendant une période limitée dans le temps dans Amazon S3, ce qui réduit encore la nécessité pour Amazon S3 de faire des demandes AWS KMS pour effectuer des opérations de chiffrement. Pour plus d'informations sur l'utilisation des clés de compartiment S3, consultez Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

Exigence du chiffrement côté serveur

Pour exiger le chiffrement côté serveur de tous les objets d'un compartiment Simple Storage Service (Amazon S3) particulier, vous pouvez utiliser une politique de compartiment. Par exemple, la politique de compartiment suivante n'autorise pas le chargement d'objet (`s3:PutObject`) si la demande n'inclut pas l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` demandant le chiffrement côté serveur avec SSE-KMS.

JSON

```
{
   "Version":"2012-10-17",
   "Id":"PutObjectPolicy",
   "Statement":[{
         "Sid":"DenyObjectsThatAreNotSSEKMS",
         "Effect":"Deny",
         "Principal":"*",
         "Action":"s3:PutObject",
```

```
            "Resource":"arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition":{
               "Null":{
                  "s3:x-amz-server-side-encryption-aws-kms-key-id":"true"
               }
            }
         }
      ]
}
```

Pour exiger qu'une donnée AWS KMS key soit utilisée pour chiffrer les objets d'un compartiment, vous pouvez utiliser la clé de `s3:x-amz-server-side-encryption-aws-kms-key-id` condition. Pour spécifier la clé KMS, vous devez utiliser une clé Amazon Resource Name (ARN) au `arn:aws:kms:`*`region`*`:`*`acct-id`*`:key/`*`key-id` format suivant. AWS Identity and Access Management ne valide pas si la chaîne pour `s3:x-amz-server-side-encryption-aws-kms-key-id` existe.

> **Note**
>
> Lorsque vous chargez un objet, vous pouvez spécifier la clé KMS à l'aide de l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` ou vous fier à la configuration de chiffrement de compartiment par défaut. Si votre PutObject demande le précise `aws:kms` dans l'`x-amz-server-side-encryption`en-tête, mais ne le `x-amz-server-side-encryption-aws-kms-key-id` précise pas, Amazon S3 part du principe que vous souhaitez utiliser le Clé gérée par AWS. Quoi qu'il en soit, l'ID de AWS KMS clé utilisé par Amazon S3 pour le chiffrement des objets doit correspondre à l'ID de AWS KMS clé indiqué dans la politique, sinon Amazon S3 refuse la demande.

Pour obtenir la liste complète des clés de condition spécifiques à Amazon S3, consultez Clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Contexte de chiffrement

Un contexte de chiffrement est un ensemble de paires valeur-clé qui contient des informations contextuelles supplémentaires sur les données. Le contexte de chiffrement n'est pas chiffré. Lorsqu'un contexte de chiffrement est spécifié pour une opération de chiffrement, Amazon S3 doit

spécifier le même contexte de chiffrement pour l'opération de déchiffrement. Dans le cas contraire, le déchiffrement échoue. AWS KMS utilise le contexte de chiffrement en tant que données authentifiées supplémentaires (AAD) pour prendre en charge le chiffrement authentifié. Pour plus d'informations sur le contexte de chiffrement, consultez Contexte de chiffrement dans le Guide du développeur AWS Key Management Service .

Par défaut, Amazon S3 utilise l'Amazon Resource Name (ARN) de l'objet ou du compartiment comme paire de contexte de chiffrement :

- Si vous utilisez SSE-KMS sans activer une clé de compartiment S3, l'ARN de l'objet est utilisé comme contexte de chiffrement.

  ```
  arn:aws:s3:::object_ARN
  ```

- Si vous utilisez SSE-KMS avec une clé de compartiment S3 activée, l'ARN du compartiment est utilisé comme contexte de chiffrement. Pour plus d'informations sur les clés de compartiment S3, consultez Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

  ```
  arn:aws:s3:::bucket_ARN
  ```

Vous pouvez éventuellement fournir une paire de contextes de chiffrement supplémentaire en utilisant l'`x-amz-server-side-encryption-context`en-tête dans une PutObject requête s3 :. Toutefois, étant donné que le contexte de chiffrement n'est pas chiffré, assurez-vous qu'il n'inclut pas d'informations sensibles. Amazon S3 stocke cette paire de clés supplémentaire avec le contexte de chiffrement par défaut. Lorsqu'il traite votre demande PUT, Amazon S3 ajoute le contexte de chiffrement par défaut d'`aws:s3:arn` à celui que vous fournissez.

Vous pouvez utiliser le contexte de chiffrement pour identifier et classer vos opérations cryptographiques par catégorie. Vous pouvez également utiliser la valeur ARN du contexte de chiffrement par défaut pour suivre les demandes pertinentes en AWS CloudTrail visualisant quel ARN Amazon S3 a été utilisé avec quelle clé de chiffrement.

Dans le `requestParameters` champ d'un fichier CloudTrail journal, le contexte de chiffrement est similaire au suivant.

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1/file_name"
}
```

Lorsque vous utilisez SSE-KMS avec la fonction de clés de compartiment S3 facultative, la valeur du contexte de chiffrement est l'ARN du compartiment.

```
"encryptionContext": {
    "aws:s3:arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
}
```

Envoi de demandes pour des objets AWS KMS chiffrés

> **Important**
>
> Toutes GET les PUT demandes d'objets AWS KMS chiffrés doivent être effectuées à l'aide du protocole SSL (Secure Sockets Layer) ou du protocole TLS (Transport Layer Security). Les demandes doivent également être signées à l'aide d'informations d'identification valides, telles que AWS Signature Version 4 (ou AWS Signature Version 2).

AWS Signature Version 4 est le processus d'ajout d'informations d'authentification aux AWS demandes envoyées par HTTP. Pour des raisons de sécurité, la plupart des demandes AWS doivent être signées avec une clé d'accès, qui consiste en un identifiant de clé d'accès et une clé d'accès secrète. Ces deux clés sont généralement appelées informations d'identification de sécurité. Pour plus d'informations, consultez Authentification des demandes (AWS Signature Version 4) et Processus de signature Signature version 4.

> **Important**
>
> Si votre objet utilise SSE-KMS, n'envoyez pas d'en-têtes de chiffrement pour les requêtes GET et HEAD. Sinon, vous obtiendrez une erreur HTTP 400 Bad Request (HTTP 400 Requête erronée).

Rubriques

- Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS)
- Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3

Spécification du chiffrement côté serveur avec AWS KMS (SSE-KMS)

Le chiffrement est configuré par défaut pour tous les compartiments Amazon S3, et tous les nouveaux objets qui sont chargés dans un compartiment S3 sont automatiquement chiffrés au repos. Le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) est la configuration de chiffrement par défaut pour chaque compartiment dans Amazon S3. Pour utiliser un autre type de chiffrement, vous pouvez soit spécifier le type de chiffrement côté serveur à utiliser dans vos PUT demandes S3, soit mettre à jour la configuration de chiffrement par défaut dans le compartiment de destination.

Si vous souhaitez spécifier un type de chiffrement différent dans vos PUT demandes, vous pouvez utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), le chiffrement double couche côté serveur avec des clés (DSSE-KMS) ou le chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C). Si vous souhaitez définir une autre configuration de chiffrement par défaut dans le compartiment de destination, vous pouvez utiliser SSE-KMS ou DSSE-KMS.

Pour plus d'informations sur la modification de la configuration de chiffrement par défaut pour vos compartiments à usage général, consultezConfiguration du chiffrement par défaut.

Lorsque vous modifiez la configuration de chiffrement par défaut de votre compartiment en SSE-KMS, le type de chiffrement des objets Amazon S3 existants dans le compartiment n'est pas modifié. Pour modifier le type de chiffrement de vos objets préexistants après avoir mis à jour la configuration de chiffrement par défaut vers SSE-KMS, vous pouvez utiliser Amazon S3 Batch Operations. Vous fournissez à S3 Batch Operations une liste d'objets, et Batch Operations appelle l'opération d'API correspondante. Vous pouvez utiliser cette Copie d'objets action pour copier des objets existants, ce qui les réécrit dans le même compartiment que les objets chiffrés SSE-KMS. Une tâche d'opérations par lots peut effectuer l'opération spécifiée sur des milliards d'objets. Pour plus d'informations, consultez Exécution d'opérations groupées sur des objets avec les opérations par lot le billet de blog sur le AWS stockage Comment chiffrer rétroactivement des objets existants dans Amazon S3 à l'aide de S3 Inventory, Amazon Athena et S3 Batch Operations.

Vous pouvez spécifier SSE-KMS à l'aide de la console Amazon S3, des opérations de l'API REST et du AWS Command Line Interface ()AWS CLI. AWS SDKs Pour plus d'informations, consultez les rubriques suivantes.

> **Note**
>
> Vous pouvez utiliser plusieurs régions AWS KMS keys dans Amazon S3. Cependant, Amazon S3 traite actuellement les clés multi-régions comme s'il s'agissait de clés à région unique et n'utilise pas les fonctions multi-régions de la clé. Pour plus d'informations, consultez Utilisation des clés multi-régions dans le Guide du développeur AWS Key Management Service .

> **Note**
>
> Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez avoir l'autorisation d'utiliser cette clé. Pour plus d'informations sur les autorisations intercomptes pour les clés KMS, consultez la section Creating KMS keys that other accounts can use (Création de clés KMS que d'autres comptes peuvent utiliser) dans le Guide du développeur AWS Key Management Service .

Utilisation de la console S3

Cette rubrique explique comment définir ou modifier le type de chiffrement d'un objet afin d'utiliser le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) à l'aide de la console Amazon S3.

> **Note**
>
> - Vous pouvez modifier le chiffrement d'un objet si sa taille est inférieure à 5 Go. Si la taille de votre objet est supérieure à 5 Go, vous devez utiliser le AWS CLIou AWS SDKspour modifier le chiffrement d'un objet.
> - Pour obtenir la liste des autorisations supplémentaires requises pour modifier le chiffrement d'un objet, consultez the section called "Autorisations requises pour les opérations d'API S3". Pour obtenir un exemple de politiques qui accorde ces autorisations, consultez the section called "Exemples de politiques basées sur l'identité".
> - Si vous modifiez le chiffrement d'un objet, un nouvel objet est créé pour remplacer l'ancien. Si la gestion des versions S3 est activée, une nouvelle version de l'objet est créée et

l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

Pour ajouter ou modifier le chiffrement d'un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments, puis l'onglet Compartiments à usage général. Accédez au compartiment ou au dossier Amazon S3 contenant les objets que vous souhaitez modifier.
3. Cochez la case correspondant aux objets à modifier.
4. Dans le menu Actions, choisissez Modifier le chiffrement côté serveur dans la liste d'options qui s'affiche.
5. Accédez à la section Chiffrement côté serveur.
6. Sous Paramètres de chiffrement, choisissez Utiliser les paramètres du compartiment pour le chiffrement par défaut ou Ignorer les paramètres du compartiment pour le chiffrement par défaut.

   > **Important**
   >
   > Si vous utilisez l'option SSE-KMS pour votre configuration de chiffrement par défaut, vous êtes soumis aux quotas RPS (demandes par seconde) de AWS KMS. Pour plus d'informations sur les quotas de AWS KMS et sur la procédure à suivre pour demander une augmentation des quotas, consultez Quotas dans le Guide du développeur AWS Key Management Service .

7. Si vous avez choisi Ignorer les paramètres de chiffrement par défaut du compartiment, configurez les paramètres de chiffrement suivants.

   a. Sous Type de chiffrement, choisissez Chiffrement côté serveur avec AWS Key Management Service clés (SSE-KMS).

   b. Sous CléAWS KMS , choisissez votre clé KMS avec l'une des options suivantes :

      - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis sélectionnez votre Clé KMS dans la liste des clés disponibles.

La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

- Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN de votre clé KMS dans le champ qui apparaît.
- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

  Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS disponibles dans le même compartiment Région AWS que le bucket. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez d'abord avoir l'autorisation d'utiliser cette clé KMS, puis saisir l'ARN de la clé KMS. Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez la section Identifying symmetric and asymmetric KMS keys (Identification des clés KMS symétriques et asymétriques) dans le Guide du développeur AWS Key Management Service .

8. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.
9. Sélectionnez Save Changes (Enregistrer les modifications).

> **Note**
>
> Cette action applique le chiffrement à tous les objets spécifiés. Lorsque vous chiffrez des dossiers, attendez la fin de l'opération d'enregistrement pour ajouter de nouveaux objets au dossier.

Utilisation de l'API REST

Lorsque vous créez un objet, à savoir, lorsque vous chargez un nouvel objet ou copiez un objet existant, vous pouvez spécifier l'utilisation du chiffrement côté serveur avec des AWS KMS keys (SSE-KMS) pour chiffrer vos données. Pour ce faire, ajoutez l'en-tête `x-amz-server-side-encryption` à la demande. Configurez la valeur de l'en-tête sur l'algorithme de chiffrement `aws:kms`. Amazon S3 confirme que l'objet est stocké grâce à SSE-KMS en renvoyant l'en-tête de réponse `x-amz-server-side-encryption`.

Si vous spécifiez l'en-tête `x-amz-server-side-encryption` avec une valeur de `aws:kms`, vous pouvez également utiliser les en-têtes de demandes suivants :

- `x-amz-server-side-encryption-aws-kms-key-id`
- `x-amz-server-side-encryption-context`
- `x-amz-server-side-encryption-bucket-key-enabled`

Rubriques

- Opérations d'API REST Amazon S3 prenant en charge SSE-KMS
- Contexte de chiffrement (x-amz-server-side-encryption-context)
- AWS KMS ID de clé (x-amz-server-side-encryption-aws-kms-key-id)
- Clés de compartiment S3 (x-amz-server-side-encryption-aws-bucket-key-enabled)

Opérations d'API REST Amazon S3 prenant en charge SSE-KMS

Les opérations d'API REST suivantes acceptent les en-têtes de demande `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id` et `x-amz-server-side-encryption-context`.

- PutObject – Lorsque vous chargez des données avec l'opération d'API PUT, vous pouvez spécifier ces en-têtes de demande.

- CopyObject – Lorsque vous copiez un objet, vous disposez d'un objet source et d'un objet cible. Lorsque vous transmettez les en-têtes SSE-KMS avec l'opération `CopyObject`, ils sont appliqués uniquement à l'objet cible. Lorsque vous copiez un objet existant, que l'objet source soit chiffré ou non, l'objet de destination n'est pas chiffré sauf si vous demandez explicitement un chiffrement côté serveur.
- POST Object – Lorsque vous utilisez une opération `POST` pour charger un objet, plutôt que des en-têtes de demande, vous fournissez les mêmes informations dans les champs du formulaire.
- CreateMultipartUpload : lorsque vous chargez des objets volumineux avec l'opération d'API de chargement partitionné, vous pouvez spécifier ces en-têtes. Vous spécifiez ces en-têtes dans la demande `CreateMultipartUpload`.

Les en-têtes de réponse des opérations d'API REST suivantes renvoient l'en-tête `x-amz-server-side-encryption` lorsqu'un objet est stocké grâce au chiffrement côté serveur.

- PutObject
- CopyObject
- POST Object
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject
- HeadObject

> **Important**
>
> - Toutes les demandes `GET` et `PUT` pour un objet protégé par AWS KMS échouent si vous ne les faites pas en utilisant le protocole SSL (Secure Sockets Layer), le protocole TLS (Transport Layer Security) ou Signature Version 4.
> - Si votre objet utilise le SSE-KMS, n'envoyez pas d'en-têtes de demande de chiffrement pour les `GET` requêtes et les `HEAD` requêtes, sinon vous obtiendrez une erreur HTTP 400. BadRequest

Contexte de chiffrement (**`x-amz-server-side-encryption-context`**)

Si vous spécifiez `x-amz-server-side-encryption:aws:kms`, l'API Simple Storage Service (Amazon S3) prend en charge un contexte de chiffrement avec l'en-tête `x-amz-server-side-encryption-context`. Un contexte de chiffrement est un ensemble de paires valeur clé qui contient des informations contextuelles supplémentaires sur les données.

Amazon S3 utilise automatiquement l'Amazon Resource Name (ARN) de l'objet ou du compartiment comme paire de contexte de chiffrement. Si vous utilisez SSE-KMS sans activer une clé de compartiment S3, vous utilisez l'ARN de l'objet comme contexte de chiffrement, par exemple, `arn:aws:s3:::`*`object_ARN`*. Toutefois, si vous utilisez SSE-KMS et activez une clé de compartiment S3, vous utilisez l'ARN du compartiment pour votre contexte de chiffrement, par exemple, `arn:aws:s3:::`*`bucket_ARN`*.

Vous pouvez éventuellement fournir une paire de contexte de chiffrement supplémentaire à l'aide de l'en-tête `x-amz-server-side-encryption-context`. Toutefois, étant donné que le contexte de chiffrement n'est pas chiffré, assurez-vous qu'il ne comprenne pas d'informations sensibles. Amazon S3 stocke cette paire de clés supplémentaire avec le contexte de chiffrement par défaut.

Pour plus d'informations sur le contexte de chiffrement dans Simple Storage Service (Amazon S3), consultez Contexte de chiffrement. Pour des informations générales sur le contexte de chiffrement, consultez la section Concepts AWS Key Management Service - Contexte de chiffrement du Guide du développeur AWS Key Management Service .

AWS KMS ID de clé (**`x-amz-server-side-encryption-aws-kms-key-id`**)

Vous pouvez utiliser l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` pour spécifier l'ID de la clé gérée par le client utilisée pour protéger les données. Si vous spécifiez l'en-tête `x-amz-server-side-encryption:aws:kms` mais que vous ne fournissez pas l'en-tête `x-amz-server-side-encryption-aws-kms-key-id`, Amazon S3 utilisera la Clé gérée par AWS (`aws/s3`) pour protéger les données. Si vous souhaitez utiliser une clé gérée par le client, vous devrez fournir l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` de la clé gérée par le client.

> **Important**
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 ne prend en charge que les clés KMS à chiffrement symétrique. Pour plus d'informations sur ces clés, consultez

Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

Clés de compartiment S3 (**`x-amz-server-side-encryption-aws-bucket-key-enabled`**)

Vous pouvez utiliser l'en-tête de demande `x-amz-server-side-encryption-aws-bucket-key-enabled` pour activer ou désactiver une clé de compartiment S3 au niveau de l'objet. Les clés de compartiment S3 réduisent les coûts de vos AWS KMS demandes en diminuant le trafic de demandes d'Amazon S3 vers AWS KMS. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

Si vous spécifiez l'en-tête `x-amz-server-side-encryption:aws:kms`, mais que vous ne fournissez pas l'en-tête `x-amz-server-side-encryption-aws-bucket-key-enabled`, votre objet utilise les paramètres de clé de compartiment S3 du compartiment de destination pour chiffrer votre objet. Pour de plus amples informations, veuillez consulter Configuration d'une clé de compartiment S3 au niveau d'un objet.

À l'aide du AWS CLI

Pour utiliser les exemples de AWS CLI commandes suivants, remplacez-les *`user input placeholders`* par vos propres informations.

Lorsque vous chargez un nouvel objet ou que vous copiez un objet existant, vous pouvez spécifier l'utilisation du chiffrement côté serveur avec des AWS KMS clés pour chiffrer vos données. Pour ce faire, ajoutez l'en-tête `--server-side-encryption aws:kms` à la demande. Utilisez le `--ssekms-key-id` *`example-key-id`* pour ajouter la AWS KMS clé gérée par le client que vous avez créée. Si vous spécifiez`--server-side-encryption aws:kms`, mais que vous ne fournissez pas d'identifiant de AWS KMS clé, Amazon S3 utilisera une clé AWS gérée.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-side-encryption aws:kms --ssekms-key-id example-key-id --body filepath
```

Vous pouvez également activer ou désactiver les clés de compartiment Amazon S3 sur vos opérations PUT ou COPY en ajoutant `--bucket-key-enabled` ou `--no-bucket-key-enabled`. Les clés de compartiment Amazon S3 peuvent réduire les coûts de vos AWS KMS demandes en diminuant le trafic de demandes d'Amazon S3 vers AWS KMS. Pour plus d'informations, consultez Reducing the cost of SSE-KMS with Amazon S3 Bucket Keys (Réduire le coût de SSE-KMS à l'aide des clés de compartiment Amazon S3).

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-
side-encryption aws:kms --bucket-key-enabled --body filepath
```

Vous pouvez chiffrer un objet non chiffré pour utiliser SSE-KMS en recopiant l'objet en place.

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --
body filepath --bucket amzn-s3-demo-bucket --key example-object-key --sse aws:kms --
sse-kms-key-id example-key-id --body filepath
```

À l'aide du AWS SDKs

Lors de l'utilisation AWS SDKs, vous pouvez demander à Amazon S3 de l'utiliser AWS KMS keys pour le chiffrement côté serveur. Les exemples suivants montrent comment utiliser SSE-KMS avec AWS SDKs pour Java et .NET. Pour plus d'informations sur les autres SDKs, consultez la section Exemples de code et de bibliothèques sur le AWS Developer Center.

> **Important**
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 ne prend en charge que les clés KMS à chiffrement symétrique. Pour plus d'informations sur ces clés, consultez Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

Opération **`CopyObject`**

Lors de la copie d'objets, vous ajoutez les mêmes propriétés de demande (`ServerSideEncryptionMethod` et `ServerSideEncryptionKeyManagementServiceKeyId`) pour demander à Amazon S3 d'utiliser une AWS KMS key. Pour plus d'informations sur la copie d'objets, consultez Copie, déplacement et changement de nom des objets.

Opération **`PUT`**

Java

Lorsque vous chargez un objet à l'aide du AWS SDK pour Java, vous pouvez demander à Amazon S3 d'utiliser un AWS KMS key en ajoutant la `SSEAwsKeyManagementParams` propriété comme indiqué dans la demande suivante :

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new SSEAwsKeyManagementParams());
```

Dans ce cas, Amazon S3 utilise le Clé gérée par AWS (`aws/s3`). Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS). Si vous le souhaitez, vous pouvez créer une clé KMS symétrique de chiffrement et la spécifier dans la demande, comme l'illustre l'exemple suivant :

```
PutObjectRequest putRequest = new PutObjectRequest(bucketName,
   keyName, file).withSSEAwsKeyManagementParams(new
 SSEAwsKeyManagementParams(keyID));
```

Pour plus d'informations sur la création de clés gérées par le client, consultez la section Programmation de l' AWS KMS API dans le Guide du AWS Key Management Service développeur.

Pour obtenir des exemples de code utilisables pour charger un objet, consultez les rubriques suivantes. Pour utiliser ces exemples, vous devez mettre à jour les exemples de code et fournir des informations de chiffrement comme illustré dans le fragment de code précédent.

- Pour charger un objet en une seule opération, consultez Chargement d'objets.
- Pour les chargements partitionnés qui utilisent les opérations d'API de chargement partitionné de haut niveau ou de bas niveau, consultez Chargement d'un objet à l'aide du chargement partitionné.

.NET

Lorsque vous chargez un objet à l'aide du AWS SDK pour .NET, vous pouvez demander à Amazon S3 d'utiliser un AWS KMS key en ajoutant la `ServerSideEncryptionMethod` propriété comme indiqué dans la demande suivante :

```
PutObjectRequest putRequest = new PutObjectRequest
 {
     BucketName = amzn-s3-demo-bucket,
     Key = keyName,
     // other properties
     ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS
 };
```

Dans ce cas, Amazon S3 utilise le Clé gérée par AWS. Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS). Si vous le souhaitez, vous pouvez créer votre propre clé symétrique de chiffrement gérée par le client et la spécifier dans la demande, comme l'illustre l'exemple suivant :

```
PutObjectRequest putRequest1 = new PutObjectRequest
{
  BucketName = amzn-s3-demo-bucket,
  Key = keyName,
  // other properties
  ServerSideEncryptionMethod = ServerSideEncryptionMethod.AWSKMS,
  ServerSideEncryptionKeyManagementServiceKeyId = keyId
};
```

Pour plus d'informations sur la création de clés gérées par le client, consultez la section Programmation de l' AWS KMS API dans le Guide du AWS Key Management Service développeur.

Pour obtenir des exemples de code utilisables pour charger un objet, consultez les rubriques suivantes. Pour utiliser ces exemples, vous devez mettre à jour les exemples de code et fournir des informations de chiffrement comme illustré dans le fragment de code précédent.

- Pour charger un objet en une seule opération, consultez Chargement d'objets.
- Pour les chargements partitionnés qui utilisent les opérations d'API de chargement partitionné de haut niveau ou de bas niveau, consultez Chargement d'un objet à l'aide du chargement partitionné.

Présigné URLs

Java

Lors de la création d'une URL pré-signée pour un objet chiffré à l'aide d'une AWS KMS key, vous devez indiquer explicitement Signature Version 4, comme l'illustre l'exemple suivant :

```
ClientConfiguration clientConfiguration = new ClientConfiguration();
clientConfiguration.setSignerOverride("AWSS3V4SignerType");
AmazonS3Client s3client = new AmazonS3Client(
        new ProfileCredentialsProvider(), clientConfiguration);
...
```

Pour obtenir un exemple de code, consultez Partage d'objets avec présigné URLs.

.NET

Lors de la création d'une URL pré-signée pour un objet chiffré à l'aide d'une AWS KMS key, vous devez indiquer explicitement Signature Version 4, comme l'illustre l'exemple suivant :

```
AWSConfigs.S3Config.UseSignatureVersion4 = true;
```

Pour obtenir un exemple de code, consultez Partage d'objets avec présigné URLs.

Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3

Les clés de compartiment Amazon S3 réduisent le coût du chiffrement côté serveur Amazon S3 avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS). L'utilisation d'une clé au niveau du compartiment pour SSE-KMS peut réduire les coûts des AWS KMS demandes jusqu'à 99 % en diminuant le trafic de demandes d'Amazon S3 vers. AWS KMS En quelques clics dans la AWS Management Console et sans modifier vos applications clients, vous pouvez configurer votre compartiment de sorte qu'il utilise une clé de compartiment S3 pour le chiffrement SSE-KMS pour les nouveaux objets.

> **Note**
>
> Les clés de compartiment S3 ne sont pas prises en charge pour le chiffrement double couche côté serveur avec des clés AWS Key Management Service (AWS KMS) (DSSE-KMS).

Clés de compartiment S3 pour SSE-KMS

Les charges de travail qui accèdent à des millions ou des milliards d'objets chiffrés avec SSE-KMS peuvent générer d'importants volumes de demandes à. AWS KMS Lorsque vous utilisez SSE-KMS pour protéger vos données sans clé de compartiment S3, Amazon S3 utilise une clé de AWS KMS données individuelle pour chaque objet. Dans ce cas, Amazon S3 effectue un appel à AWS KMS chaque fois qu'une demande est faite contre un objet chiffré par KMS. Pour plus d'informations sur le fonctionnement de SSE-KMS, consultez Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

Lorsque vous configurez votre compartiment pour utiliser une clé de compartiment S3 pour SSE-KMS, vous AWS générez une clé de type bucket de courte durée à partir de AWS KMS, puis la

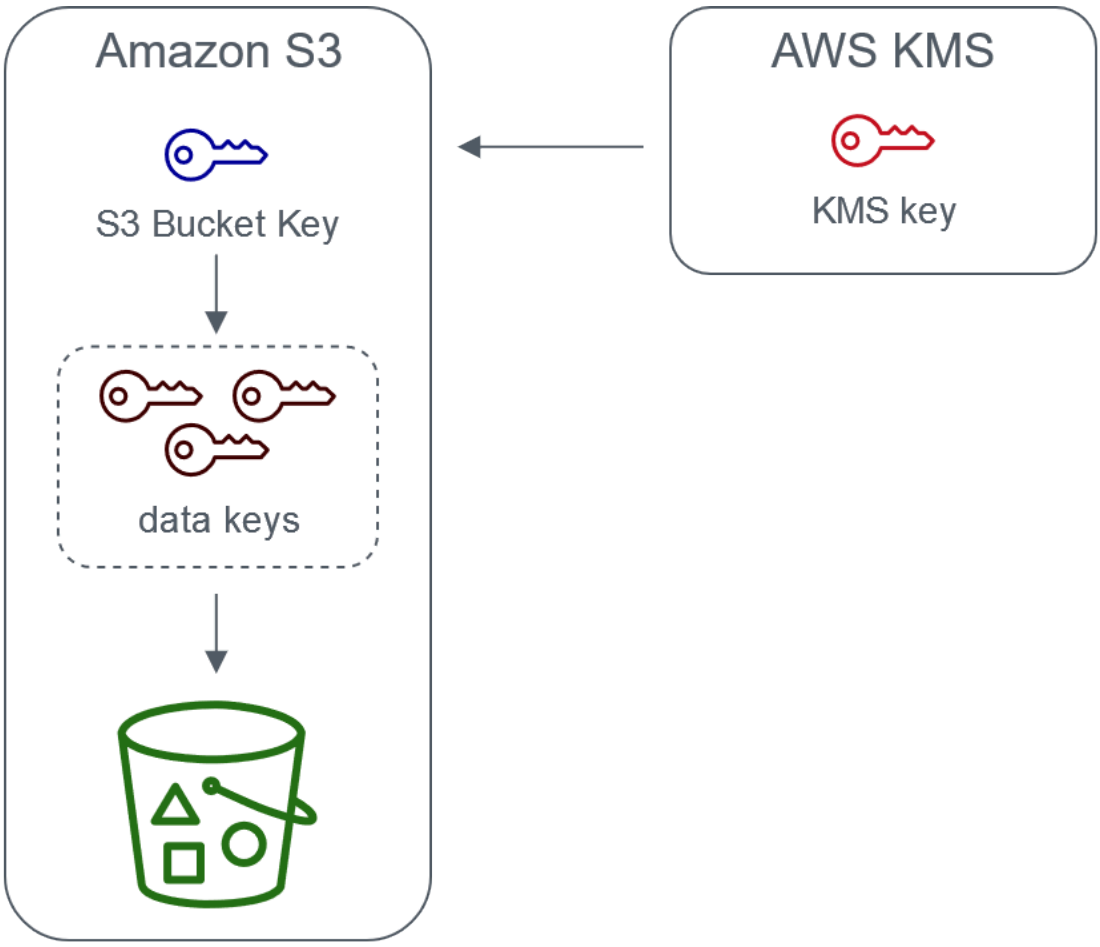
conservez temporairement dans S3. Cette clé de niveau compartiment créera des clés de données pour les nouveaux objets au cours de son cycle de vie. Les clés de compartiment S3 sont utilisées pendant une période limitée dans Amazon S3, ce qui réduit la nécessité pour S3 de faire des demandes AWS KMS pour effectuer des opérations de chiffrement. Cela permet de réduire le trafic de S3 à S3 AWS KMS, ce qui vous permet d'accéder à des objets AWS KMS chiffrés dans Amazon S3 à une fraction du coût précédent.

Les clés uniques au niveau du compartiment sont récupérées au moins une fois par demandeur afin de garantir que l'accès du demandeur à la clé est capturé lors d'un événement. AWS KMS CloudTrail Amazon S3 traite les appelants comme des demandeurs différents lorsqu'ils utilisent des rôles ou des comptes différents, ou lorsqu'ils utilisent le même rôle avec des politiques de cadrage différentes. AWS KMS les économies de demandes reflètent le nombre de demandeurs, les modèles de demandes et l'âge relatif des objets demandés. Par exemple, un nombre réduit de demandeurs, sollicitant plusieurs objets dans une fenêtre de temps limitée, et chiffrés avec la même clé au niveau des compartiments, permettra de réaliser des économies plus importantes.

> **Note**
>
> L'utilisation de clés de compartiment S3 vous permet de réduire les coûts liés aux AWS KMS demandes en réduisant le nombre de demandes à AWS KMS for `Encrypt` et les `Decrypt` opérations grâce à l'utilisation d'une clé au niveau du compartiment. `GenerateDataKey` De par leur conception, les demandes ultérieures qui tirent parti de cette clé au niveau du compartiment n'entraînent pas de demandes d' AWS KMS API et ne valident pas l'accès par rapport à la politique de AWS KMS clé.

Lorsque vous configurez une clé de compartiment S3, les objets qui se trouvent déjà dans le compartiment n'utilisent pas la clé de compartiment S3. Pour configurer une clé de compartiment S3 pour des objets existants, vous pouvez utiliser une opération `CopyObject`. Pour de plus amples informations, veuillez consulter Configuration d'une clé de compartiment S3 au niveau d'un objet.

Amazon S3 partage une clé de compartiment S3 uniquement pour les objets chiffrés avec la même AWS KMS key. Les clés de compartiment S3 sont compatibles avec les clés KMS créées par AWS KMS, le matériel clé importé et le matériel clé soutenu par des magasins de clés personnalisés.



Server-side encryption with AWS Key Management service using an S3 Bucket Key

Configuration de clés de compartiment S3

Vous pouvez configurer votre compartiment pour utiliser une clé de compartiment S3 pour SSE-KMS sur de nouveaux objets via la console Amazon S3 ou l' AWS SDKsAPI AWS CLI REST. Lorsque l'option « S3 Bucket Keys » (Clés du compartiment S3) est activée sur votre compartiment, les objets chargés avec une autre clé SSE-KMS spécifiée utiliseront leur propres clés du compartiment S3. Quel que soit votre paramètre de clé de compartiment S3, vous pouvez inclure l'en-tête `x-amz-server-side-encryption-bucket-key-enabled` avec une valeur `true` ou `false` dans votre requête, afin de remplacer le paramètre de compartiment.

Avant de configurer votre compartiment de sorte qu'il utilise une clé de compartiment S3, consultez Modifications à prendre en compte avant d'activer une clé de compartiment S3.

Configuration d'une clé de compartiment S3 à l'aide de la console Amazon S3

Lorsque vous créez un nouveau compartiment, vous pouvez configurer votre compartiment de sorte qu'il utilise une clé de compartiment S3 pour SSE-KMS sur de nouveaux objets. Vous pouvez également configurer un compartiment existant de sorte qu'il utilise une clé de compartiment S3 pour SSE-KMS sur de nouveaux objets en mettant à jour vos propriétés de compartiment.

Pour de plus amples informations, veuillez consulter Configuration de votre compartiment de sorte qu'il utilise une clé de compartiment S3 avec SSE-KMS pour de nouveaux objets.

Support de l'API REST et du AWS SDK pour les clés de compartiment S3 AWS CLI

Vous pouvez utiliser l'API REST ou le AWS SDK pour configurer votre compartiment afin qu'il utilise une clé de compartiment S3 pour SSE-KMS sur de nouveaux objets. AWS CLI Vous pouvez également activer une clé de compartiment S3 au niveau de l'objet.

Pour de plus amples informations, consultez les ressources suivantes :

- Configuration d'une clé de compartiment S3 au niveau d'un objet
- Configuration de votre compartiment de sorte qu'il utilise une clé de compartiment S3 avec SSE-KMS pour de nouveaux objets

Les opérations d'API suivantes prennent en charge les clés de compartiment S3 pour SSE-KMS :

- PutBucketEncryption
  - `ServerSideEncryptionRule` accepte le `BucketKeyEnabled` paramètre permettant d'activer et de désactiver une clé de compartiment S3.
- GetBucketEncryption
  - `ServerSideEncryptionRule` renvoie les paramètres de `BucketKeyEnabled`.
- PutObject, CopyObjectCreateMultipartUpload, et objet POST
  - L'en-tête de demande `x-amz-server-side-encryption-bucket-key-enabled` active ou désactive une clé de compartiment S3 au niveau de l'objet.
- HeadObject, GetObject, UploadPartCopy, UploadPart, et CompleteMultipartUpload
  - L'en-tête de réponse `x-amz-server-side-encryption-bucket-key-enabled` indique si une clé de compartiment S3 est activée ou désactivée pour un objet.

Travailler avec AWS CloudFormation

Dans AWS CloudFormation, la `AWS::S3::Bucket` ressource inclut une propriété de chiffrement appelée `BucketKeyEnabled` que vous pouvez utiliser pour activer ou désactiver une clé de compartiment S3.

Pour de plus amples informations, veuillez consulter En utilisant AWS CloudFormation.

Modifications à prendre en compte avant d'activer une clé de compartiment S3

Avant d'activer une clé de compartiment S3, notez les modifications suivantes :

IAM ou politiques AWS KMS clés

Si vos politiques AWS Identity and Access Management (IAM) ou AWS KMS clés existantes utilisent votre objet Amazon Resource Name (ARN) comme contexte de chiffrement pour affiner ou limiter l'accès à votre clé KMS, ces politiques ne fonctionneront pas avec une clé de compartiment S3. Les clés de compartiment S3 utilisent l'ARN du compartiment comme contexte de chiffrement. Avant d'activer une clé de compartiment S3, mettez à jour vos politiques IAM ou vos politiques AWS KMS clés pour utiliser l'ARN de votre compartiment comme contexte de chiffrement.

Pour plus d'informations sur le contexte de chiffrement et les clés de compartiment S3, consultez Contexte de chiffrement.

CloudTrail événements pour AWS KMS

Une fois que vous avez activé une clé de compartiment S3, vos AWS KMS CloudTrail événements enregistrent l'ARN de votre compartiment au lieu de l'ARN de votre objet. En outre, vous voyez moins d' CloudTrail événements KMS pour les objets SSE-KMS dans vos journaux. Les informations clés étant limitées dans le temps dans Amazon S3, moins de demandes sont adressées à AWS KMS.

Utilisation d'une clé de compartiment S3 avec réplication

Vous pouvez utiliser des clés de compartiment S3 avec la réplication dans la même Région (SRR) et la réplication entre Régions (CRR).

Lorsqu'Amazon S3 réplique un objet chiffré, il conserve généralement les paramètres de chiffrement de l'objet réplica dans le compartiment de destination. Toutefois, si l'objet source n'est pas chiffré et que votre compartiment de destination utilise un chiffrement par défaut ou une clé de compartiment S3, Amazon S3 chiffre l'objet avec la configuration du compartiment de destination.

Les exemples suivants illustrent le fonctionnement d'une clé de compartiment S3 avec la réplication. Pour plus d'informations, consultez Réplication d'objets chiffrés (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

Example Exemple 1 : l'objet source utilise des clés de compartiment S3, le compartiment de destination utilise le chiffrement par défaut

Si votre objet source utilise une clé de compartiment S3 mais que votre compartiment de destination utilise le chiffrement par défaut avec SSE-KMS, l'objet réplica conserve ses paramètres de chiffrement de clé de compartiment S3 dans le compartiment de destination. Le compartiment de destination utilise toujours le chiffrement par défaut avec SSE-KMS.

Example Exemple 2 : l'objet source n'est pas chiffré, le compartiment de destination utilise une clé de compartiment S3 avec SSE-KMS

Si votre objet source n'est pas chiffré et que le compartiment de destination utilise une clé de compartiment S3 avec SSE-KMS, l'objet de réplica est chiffré avec une clé de compartiment S3 utilisant SSE-KMS dans le compartiment de destination. Cela produit un `ETag` de l'objet source différent de l'`ETag` de l'objet réplica. Vous devez mettre à jour les applications qui utilisent le `ETag` pour compenser cette différence.

Utilisation des clés de compartiment S3

Pour plus d'informations sur l'activation et l'utilisation des clés de compartiment S3, consultez les sections suivantes :

- Configuration de votre compartiment de sorte qu'il utilise une clé de compartiment S3 avec SSE-KMS pour de nouveaux objets
- Configuration d'une clé de compartiment S3 au niveau d'un objet
- Affichage des paramètres d'une clé de compartiment S3

Configuration de votre compartiment de sorte qu'il utilise une clé de compartiment S3 avec SSE-KMS pour de nouveaux objets

Lorsque vous configurez le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), vous pouvez configurer votre compartiment pour utiliser une clé de compartiment S3 pour SSE-KMS sur de nouveaux objets. Les clés de compartiment S3 réduisent le trafic de requêtes en provenance d'Amazon S3 AWS KMS et réduisent le coût du SSE-KMS. Pour

de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

Vous pouvez configurer votre compartiment pour utiliser une clé de compartiment S3 pour SSE-KMS sur de nouveaux objets à l'aide de la console Amazon S3, de l'API REST, AWS SDKs, AWS Command Line Interface (AWS CLI) ou. AWS CloudFormation Si vous souhaitez activer ou désactiver une clé de compartiment S3 pour des objets existants, vous pouvez utiliser une opération `CopyObject`. Pour plus d'informations, consultez Configuration d'une clé de compartiment S3 au niveau d'un objet et Utilisation des opérations par lot pour activer les clés de compartiment S3 pour SSE-KMS.

Lorsqu'une clé de compartiment S3 est activée pour le compartiment source ou de destination, le contexte de chiffrement est l'Amazon Resource Name (ARN) du compartiment source et non l'ARN de l'objet, par exemple, `arn:aws:s3:::`*`bucket_ARN`*. Vous devez mettre à jour vos politiques IAM pour utiliser l'ARN du compartiment comme contexte de chiffrement. Pour plus d'informations, consultez Clés de compartiment S3 et réplication.

Les exemples suivants illustrent le fonctionnement d'une clé de compartiment S3 avec la réplication. Pour plus d'informations, consultez Réplication d'objets chiffrés (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

Prérequis

Avant de configurer votre compartiment de sorte qu'il utilise une clé de compartiment S3, consultez Modifications à prendre en compte avant d'activer une clé de compartiment S3.

Utiliser la console S3.

Dans la console S3, vous pouvez activer ou désactiver une clé de compartiment S3 pour un nouveau compartiment ou un compartiment existant. Les objets de la console S3 conservent le paramètre de clé de compartiment S3 présent dans la configuration du compartiment. Lorsque vous activez une clé de compartiment S3 pour votre compartiment, les nouveaux objets que vous chargez dans le compartiment utilisent une clé de compartiment S3 pour SSE-KMS.

Chargement, copie ou modification d'objets dans des compartiments pour lesquels une clé de compartiment S3 est activée

Si vous chargez, modifiez ou copiez un objet dans un compartiment pour lequel une clé de compartiment S3 est activée, les paramètres de clé de compartiment S3 de cet objet peuvent être mis à jour pour les aligner sur la configuration du compartiment.

Si une clé de compartiment S3 est déjà activée pour un objet, les paramètres de clé de compartiment S3 de cet objet ne changent pas lorsque vous copiez ou modifiez l'objet. Toutefois, si vous modifiez ou copiez un objet pour lequel aucune clé de compartiment S3 n'est activée et que le compartiment de destination a une configuration de clé de compartiment S3, l'objet conserve les paramètres de clé de compartiment S3 du compartiment de destination. Par exemple, si aucune clé de compartiment S3 n'est activée pour votre objet source, mais que la clé de compartiment S3 est activée pour le compartiment de destination, une clé de compartiment S3 est activée pour l'objet.

Pour activer une clé de compartiment S3 lorsque vous créez un nouveau compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Choisissez Créer un compartiment.
4. Entrez le nom de votre compartiment, puis choisissez votre Région AWS.
5. Sous Chiffrement par défaut, pour Type de clé de chiffrement, choisissez CléAWS Key Management Service (SSE-KMS).
6. Sous CléAWS KMS , choisissez votre clé KMS avec l'une des options suivantes :

   - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans la liste des clés disponibles.

     La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez la section Clés et AWS clés client dans le Guide du AWS Key Management Service développeur.
   - Pour saisir l'ARN de la clé KMS, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de votre clé KMS dans le champ qui s'affiche.
   - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

     Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.
7. Sous Clé de compartiment, choisissez Activer.
8. Choisissez Créer un compartiment.

   Amazon S3 crée votre compartiment avec une clé de compartiment S3 activée. Les nouveaux objets que vous chargez dans le compartiment utiliseront une clé de compartiment S3.

Pour désactiver une clé de compartiment S3, suivez les étapes précédentes et choisissez Désactiver.

Pour activer une clé de compartiment S3 pour un compartiment existant

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le compartiment pour lequel vous souhaitez activer une clé de compartiment S3.
4. Choisissez l'onglet Propriétés.
5. Sous Default encryption (Chiffrement par défaut), choisissez Edit (Modifier).
6. Sous Chiffrement par défaut, pour Type de clé de chiffrement, choisissez CléAWS Key Management Service (SSE-KMS).
7. Sous CléAWS KMS , choisissez votre clé KMS avec l'une des options suivantes :

   - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis choisissez votre clé KMS dans la liste des clés disponibles.

     La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez la section Clés et AWS clés client dans le Guide du AWS Key Management Service développeur.
   - Pour saisir l'ARN de la clé KMS, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de votre clé KMS dans le champ qui s'affiche.
   - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

     Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.
8. Sous Clé de compartiment, choisissez Activer.
9. Sélectionnez Save Changes (Enregistrer les modifications).

   Amazon S3 active une clé de compartiment S3 pour les nouveaux objets ajoutés à votre compartiment. Les objets existants n'utilisent pas la clé de compartiment S3. Pour configurer une clé de compartiment S3 pour des objets existants, vous pouvez utiliser une opération

`CopyObject`. Pour plus d'informations, consultez Configuration d'une clé de compartiment S3 au niveau d'un objet.

Pour désactiver une clé de compartiment S3, suivez les étapes précédentes et choisissez Désactiver.

Utilisation de l'API REST

Vous pouvez l'utiliser PutBucketEncryptionpour activer ou désactiver une clé de compartiment S3 pour votre compartiment. Pour configurer une clé de compartiment S3 avec`PutBucketEncryption`, utilisez le type de ServerSideEncryptionRuledonnées, qui inclut le chiffrement par défaut avec SSE-KMS. Vous pouvez également utiliser une clé gérée par le client en indiquant l'ID de clé KMS de la clé gérée par le client.

Pour plus d'informations et des exemples de syntaxe, consultez PutBucketEncryption.

Utilisation du AWS SDK pour Java

L'exemple suivant active le chiffrement du compartiment par défaut avec SSE-KMS et une clé de compartiment S3 à l'aide d' AWS SDK pour Java.

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

ServerSideEncryptionByDefault serverSideEncryptionByDefault = new
 ServerSideEncryptionByDefault()
    .withSSEAlgorithm(SSEAlgorithm.KMS);
ServerSideEncryptionRule rule = new ServerSideEncryptionRule()
    .withApplyServerSideEncryptionByDefault(serverSideEncryptionByDefault)
    .withBucketKeyEnabled(true);
ServerSideEncryptionConfiguration serverSideEncryptionConfiguration =
    new ServerSideEncryptionConfiguration().withRules(Collections.singleton(rule));

SetBucketEncryptionRequest setBucketEncryptionRequest = new
 SetBucketEncryptionRequest()
    .withServerSideEncryptionConfiguration(serverSideEncryptionConfiguration)
    .withBucketName(bucketName);
```

```
s3client.setBucketEncryption(setBucketEncryptionRequest);
```

À l'aide du AWS CLI

L'exemple suivant active le chiffrement du compartiment par défaut avec SSE-KMS et une clé de compartiment S3 à l'aide d' AWS CLI. Remplacez *user input placeholders* par vos propres informations.

```
aws s3api put-bucket-encryption --bucket amzn-s3-demo-bucket --server-side-encryption-
configuration '{
        "Rules": [
            {
                "ApplyServerSideEncryptionByDefault": {
                    "SSEAlgorithm": "aws:kms",
                    "KMSMasterKeyID": "KMS-Key-ARN"
                },
                "BucketKeyEnabled": true
            }
        ]
    }'
```

En utilisant AWS CloudFormation

Pour plus d'informations sur la configuration d'une clé de compartiment S3 avec AWS CloudFormation, consultez AWS::S3::Bucket ServerSideEncryptionRulele guide de AWS CloudFormation l'utilisateur.

Configuration d'une clé de compartiment S3 au niveau d'un objet

Lorsque vous effectuez une opération PUT ou COPY à l'aide de l'API REST AWS SDKs AWS CLI, ou, vous pouvez activer ou désactiver une clé de compartiment S3 au niveau de l'objet en ajoutant l'en-tête de `x-amz-server-side-encryption-bucket-key-enabled` demande avec une `false` valeur `true` ou. Les clés de compartiment S3 réduisent le coût du chiffrement côté serveur à l'aide de AWS Key Management Service (AWS KMS) (SSE-KMS) en diminuant le trafic de requêtes d'Amazon S3 vers. AWS KMS Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

Lorsque vous configurez une clé de compartiment S3 pour un objet à l'aide d'une opération PUT ou COPY, Amazon S3 met à jour uniquement les paramètres de cet objet. Les paramètres de clé

de compartiment S3 pour le compartiment de destination ne changent pas. Si vous soumettez une requête PUT ou COPY pour un objet chiffré par KMS dans un compartiment avec l'option « S3 Bucket Keys » (Clés du compartiment S3) activée, votre opération au niveau de l'objet utilisera automatiquement cette option à moins que vous ne désactiviez les clés dans l'en-tête de la requête. Si vous ne spécifiez pas de clé de compartiment S3 pour votre objet, Amazon S3 applique les paramètres de clé de compartiment S3 du compartiment de destination à l'objet.

Prérequis :

Avant de configurer votre objet de sorte qu'il utilise une clé de compartiment S3, consultez Modifications à prendre en compte avant d'activer une clé de compartiment S3.

Rubriques

- Opérations par lot Amazon S3
- Utilisation de l'API REST
- Utilisation du AWS SDK pour Java PutObject ()
- En utilisant le AWS CLI (PutObject)

Opérations par lot Amazon S3

Pour chiffrer vos objets Amazon S3 existants, vous pouvez utiliser des opérations par lot Amazon S3. Vous fournissez à la fonctionnalité d'opérations par lot S3 une liste d'objets sur lesquels agir. La fonctionnalité d'opérations par lot appelle l'API correspondante pour exécuter l'opération spécifiée.

Vous pouvez utiliser l'opération de copie des opérations par lot S3 pour copier des objets non chiffrés existants et les réécrire dans le même compartiment en tant qu'objets chiffrés. Une tâche d'opérations par lot peut effectuer l'opération spécifiée sur des milliards d'objets. Pour plus d'informations, consultez Exécution d'opérations groupées sur des objets avec les opérations par lot et le billet de blog Encrypting objects with Amazon S3 Batch Operations.

Utilisation de l'API REST

Lorsque vous utilisez SSE-KMS, vous pouvez activer une clé de compartiment S3 pour un objet à l'aide des opérations d'API suivantes :

- PutObject— Lorsque vous chargez un objet, vous pouvez spécifier l'en-tête de `x-amz-server-side-encryption-bucket-key-enabled` demande pour activer ou désactiver une clé de compartiment S3 au niveau de l'objet.

- CopyObject— Lorsque vous copiez un objet et configurez SSE-KMS, vous pouvez spécifier l'en-tête de `x-amz-server-side-encryption-bucket-key-enabled` demande pour activer ou désactiver une clé de compartiment S3 pour votre objet.
- POST Object : lorsque vous utilisez une opération `POST` pour charger un objet et configurer SSE-KMS, vous pouvez utiliser le champ de formulaire `x-amz-server-side-encryption-bucket-key-enabled` pour activer ou désactiver une clé de compartiment S3 pour votre objet.
- CreateMultipartUpload— Lorsque vous chargez des objets volumineux à l'aide de l'opération `CreateMultipartUpload` API et que vous configurez SSE-KMS, vous pouvez utiliser l'en-tête de `x-amz-server-side-encryption-bucket-key-enabled` demande pour activer ou désactiver une clé de compartiment S3 pour votre objet.

Pour activer une clé de compartiment S3 au niveau de l'objet, incluez l'en-tête de demande `x-amz-server-side-encryption-bucket-key-enabled`. Pour plus d'informations sur SSE-KMS et l'API REST, consultez Utilisation de l'API REST.

Utilisation du AWS SDK pour Java PutObject ()

Vous pouvez utiliser l'exemple suivant pour configurer une clé de compartiment S3 au niveau de l'objet à l'aide du kit AWS SDK pour Java.

Java

```
AmazonS3 s3client = AmazonS3ClientBuilder.standard()
    .withRegion(Regions.DEFAULT_REGION)
    .build();

String bucketName = "amzn-s3-demo-bucket1";
String keyName = "key name for object";
String contents = "file contents";

PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName, keyName,
 contents)
    .withBucketKeyEnabled(true);

s3client.putObject(putObjectRequest);
```

En utilisant le AWS CLI (PutObject)

Vous pouvez utiliser l' AWS CLI exemple suivant pour configurer une clé de compartiment S3 au niveau de l'objet dans le cadre d'une `PutObject` demande.

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key object key name --server-side-encryption aws:kms --bucket-key-enabled --body filepath
```

Affichage des paramètres d'une clé de compartiment S3

Vous pouvez consulter les paramètres d'une clé de compartiment S3 au niveau du compartiment ou de l'objet à l'aide de la console Amazon S3, de l'API REST, AWS Command Line Interface (AWS CLI) ou AWS SDKs.

Les clés de compartiment S3 réduisent le trafic de requêtes en provenance d'Amazon S3 vers Amazon S3 AWS KMS et réduisent le coût du chiffrement côté serveur AWS Key Management Service (SSE-KMS). Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.

Pour afficher les paramètres de clé de compartiment S3 d'un compartiment ou d'un objet ayant conservé les paramètres de clé de compartiment S3 présents dans la configuration du compartiment, vous devez obtenir l'autorisation d'effectuer l'action `s3:GetEncryptionConfiguration`. Pour plus d'informations, consultez GetBucketEncryption dans la Référence d'API Amazon Simple Storage Service.

Utilisation de la console S3

Dans la console S3, vous pouvez afficher les paramètres de clé de compartiment S3 pour votre compartiment ou votre objet. Les paramètres de clé de compartiment S3 sont issus de la configuration du compartiment, sauf si une clé de compartiment S3 est déjà configurée pour les objets source.

Les objets et les dossiers dans le même compartiment peuvent avoir des paramètres de clé de compartiment S3 différents. Par exemple, si vous chargez un objet à l'aide de l'API REST et que vous activez une clé de compartiment S3 pour l'objet, l'objet conserve son paramètre de clé de compartiment S3 dans le compartiment de destination, même si la clé de compartiment S3 est désactivée dans le compartiment de destination. Autre exemple, si vous activez une clé de compartiment S3 pour un compartiment existant, les objets qui se trouvent déjà dans le compartiment n'utilisent pas de clé de compartiment S3. Toutefois, une clé de compartiment S3 est activée pour les nouveaux objets.

Pour afficher le paramètre de clé de compartiment S3 pour votre compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le compartiment pour lequel vous souhaitez activer une clé de compartiment S3.
4. Choisissez Propriétés.
5. Dans la section Chiffrement par défaut, sous Clé de compartiment, vous voyez le paramètre de clé de compartiment S3 pour votre compartiment.

   Si le paramètre de clé de compartiment S3 ne s'affiche pas, il se peut que vous n'ayez pas l'autorisation d'exécuter l'action `s3:GetEncryptionConfiguration`. Pour plus d'informations, consultez GetBucketEncryption dans la Référence d'API Amazon Simple Storage Service.

Pour afficher le paramètre de clé de compartiment S3 pour votre objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le compartiment pour lequel vous souhaitez activer une clé de compartiment S3.
3. Dans la liste Objets, choisissez le nom de votre objet.
4. Sous l'onglet Détails, sous Paramètres de chiffrement côté serveur, choisissez Modifier.

   Sous Clé de compartiment, vous voyez le paramètre de clé de compartiment S3 pour votre objet. Vous ne pouvez pas modifier ce paramètre.

À l'aide du AWS CLI

Pour renvoyer les paramètres de clé de compartiment S3 au niveau du compartiment

Pour utiliser cet exemple, remplacez chaque *`user input placeholder`* par vos propres informations.

```
aws s3api get-bucket-encryption --bucket amzn-s3-demo-bucket1
```

Pour plus d'informations, consultez get-bucket-encryption dans la Référence des commandes de l'AWS CLI .

Pour renvoyer les paramètres au niveau de l'objet pour une clé de compartiment S3

Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

```
aws s3api head-object --bucket amzn-s3-demo-bucket1 --key my_images.tar.bz2
```

Pour plus d'informations, consultez head-object dans la Référence des commandes de l'AWS CLI .

Utilisation de l'API REST

Pour renvoyer les paramètres de clé de compartiment S3 au niveau du compartiment

Pour renvoyer des informations de chiffrement pour un compartiment, y compris les paramètres d'une clé de compartiment S3, utilisez l'opération `GetBucketEncryption`. Les paramètres de clé de compartiment S3 sont renvoyés dans le corps de la réponse dans l'élément `ServerSideEncryptionConfiguration` avec le paramètre `BucketKeyEnabled`. Pour plus d'informations, consultez GetBucketEncryption dans la Référence d'API Amazon S3.

Pour renvoyer les paramètres au niveau de l'objet pour une clé de compartiment S3

Pour renvoyer l'état Clé de compartiment S3 d'un objet, utilisez l'opération `HeadObject`. `HeadObject` renvoie l'en-tête de réponse `x-amz-server-side-encryption-bucket-key-enabled` pour indiquer si une clé de compartiment S3 est activée ou désactivée pour l'objet. Pour plus d'informations, consultez HeadObject dans la Référence d'API Amazon S3.

Les opérations d'API suivantes retournent également l'en-tête de réponse `x-amz-server-side-encryption-bucket-key-enabled` si une clé de compartiment S3 est configurée pour un objet :

- PutObject
- PostObject
- CopyObject
- CreateMultipartUpload
- UploadPartCopy
- UploadPart
- CompleteMultipartUpload
- GetObject

Utilisation du chiffrement double couche côté serveur avec AWS KMS clés (DSSE-KMS)

L'utilisation du chiffrement double couche côté serveur avec des clés AWS Key Management Service (AWS KMS) (DSSE-KMS) applique deux couches de chiffrement aux objets lorsqu'ils sont chargés sur Amazon S3. DSSE-KMS vous permet de satisfaire plus facilement aux normes de conformité, qui vous imposent d'appliquer un chiffrement multicouche à vos données et de contrôler entièrement vos clés de chiffrement.

Lorsque vous utilisez le DSSE-KMS avec un compartiment Amazon S3, les AWS KMS clés doivent se trouver dans la même région que le compartiment. De même, lorsqu'un chiffrement DSSE-KMS est demandé pour l'objet, le total de contrôle S3, qui fait partie des métadonnées de l'objet, est stocké sous une forme chiffrée. Pour en savoir plus sur le total de contrôle, consultez Vérification de l'intégrité des objets dans Amazon S3.

L'utilisation de DSSE-KMS et. AWS KMS keys Pour en savoir plus sur la tarification de DSSE-KMS, consultez Concepts de AWS KMS key dans le Guide du développeur AWS Key Management Service et Tarification AWS KMS.

> **Note**
>
> Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS.

Nécessite un chiffrement double couche côté serveur avec AWS KMS keys (DSSE-KMS)

Pour exiger un chiffrement double couche côté serveur de tous les objets contenus dans un compartiment Amazon S3 déterminé, vous pouvez utiliser une politique de compartiment. Par exemple, la politique de compartiment suivante n'autorise pas le chargement d'objet (`s3:PutObject`) si la demande n'inclut pas d'en-tête `x-amz-server-side-encryption` demandant un chiffrement côté serveur avec DSSE-KMS.

JSON

```
{
            "Version":"2012-10-17",
            "Id":"PutObjectPolicy",
            "Statement":[{
                  "Sid":"DenyUnEncryptedObjectUploads",
```

```
                "Effect":"Deny",
                "Principal":"*",
                "Action":"s3:PutObject",
                "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
                "Condition":{
                   "StringNotEquals":{
                      "s3:x-amz-server-side-encryption":"aws:kms:dsse"
                   }
                }
             }
          ]
       }
```

Rubriques

- Spécification du chiffrement double couche côté serveur avec des clés AWS KMS (DSSE-KMS)

Spécification du chiffrement double couche côté serveur avec des clés AWS KMS (DSSE-KMS)

Vous pouvez appliquer le chiffrement lorsque vous chargez un nouvel objet ou copiez un objet existant.

Vous pouvez spécifier DSSE-KMS en utilisant la console Amazon S3, l'API REST Amazon S3 et l' AWS Command Line Interface (AWS CLI). Pour plus d'informations, consultez les rubriques suivantes.

> **Note**
>
> Vous pouvez utiliser plusieurs régions AWS KMS keys dans Amazon S3. Cependant, Amazon S3 traite actuellement les clés multi-régions comme s'il s'agissait de clés à région unique et n'utilise pas les fonctions multi-régions de la clé. Pour plus d'informations, consultez Utilisation des clés multi-régions dans le Guide du développeur AWS Key Management Service .

> **Note**
>
> Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez avoir l'autorisation d'utiliser la clé. Pour plus d'informations sur les autorisations intercomptes pour les clés KMS, consultez la section Creating KMS keys that other accounts can use (Création

de clés KMS que d'autres comptes peuvent utiliser) dans le Guide du développeur AWS Key Management Service .

Utilisation de la console S3

Cette section explique comment définir ou modifier le type de chiffrement d'un objet afin d'utiliser un chiffrement double couche côté serveur avec des clés AWS Key Management Service (AWS KMS) (DSSE-KMS) à l'aide de la console Amazon S3.

> **Note**
>
> - Vous pouvez modifier le chiffrement d'un objet si sa taille est inférieure à 5 Go. Si la taille de votre objet est supérieure à 5 Go, vous devez utiliser le AWS CLIou AWS SDKspour modifier le chiffrement d'un objet.
> - Pour obtenir la liste des autorisations supplémentaires requises pour modifier le chiffrement d'un objet, consultez the section called "Autorisations requises pour les opérations d'API S3". Pour obtenir un exemple de politiques qui accorde ces autorisations, consultez the section called "Exemples de politiques basées sur l'identité".
> - Si vous modifiez le chiffrement d'un objet, un nouvel objet est créé pour remplacer l'ancien. Si la gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

Pour ajouter ou modifier le chiffrement d'un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Compartiments, puis l'onglet Compartiments à usage général. Accédez au compartiment ou au dossier Amazon S3 contenant les objets que vous souhaitez modifier.
3. Cochez la case correspondant aux objets à modifier.
4. Dans le menu Actions, choisissez Modifier le chiffrement côté serveur dans la liste d'options qui s'affiche.
5. Accédez à la section Chiffrement côté serveur.

6. Sous Paramètres de chiffrement, choisissez Utiliser les paramètres du compartiment pour le chiffrement par défaut ou Ignorer les paramètres du compartiment pour le chiffrement par défaut.
7. Si vous avez choisi Ignorer les paramètres de chiffrement par défaut du compartiment, configurez les paramètres de chiffrement suivants.

   a. Sous Type de chiffrement, choisissez Chiffrement double couche côté serveur avec AWS Key Management Service clés (DSSE-KMS).

   b. Sous CléAWS KMS , choisissez votre clé KMS avec l'une des options suivantes :

   - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS keys, puis sélectionnez votre Clé KMS dans la liste des clés disponibles.

     La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .
   - Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN de votre clé KMS dans le champ qui apparaît.
   - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

     Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous pouvez uniquement utiliser des clés KMS disponibles dans la même Région AWS que le compartiment. La console Amazon S3 répertorie uniquement les 100 premières clés KMS dans la même région que le compartiment. Pour utiliser une clé KMS qui n'est pas répertoriée, vous devez saisir l'ARN de votre clé KMS. Si vous souhaitez utiliser une clé KMS qui appartient à un autre compte, vous devez d'abord avoir l'autorisation d'utiliser cette clé, puis vous devez saisir l'ARN de la clé KMS.
>
> Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations,

consultez Identification des clés KMS asymétriques dans le Guide du développeur AWS Key Management Service .

8. Pour Clé de compartiment, choisissez Désactiver. Les clés de compartiment S3 ne sont pas prises en charge pour DSSE-KMS.
9. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.
10. Sélectionnez Save Changes (Enregistrer les modifications).

> **Note**
>
> Cette action applique le chiffrement à tous les objets spécifiés. Lorsque vous chiffrez des dossiers, attendez la fin de l'opération d'enregistrement pour ajouter de nouveaux objets au dossier.

Utilisation de l'API REST

Lorsque vous créez un objet, c'est-à-dire lorsque vous téléchargez un nouvel objet ou que vous copiez un objet existant, vous pouvez spécifier l'utilisation du chiffrement double couche côté serveur AWS KMS keys (DSSE-KMS) pour chiffrer vos données. Pour ce faire, ajoutez l'en-tête `x-amz-server-side-encryption` à la demande. Configurez la valeur de l'en-tête sur l'algorithme de chiffrement `aws:kms:dsse`. Amazon S3 confirme que votre objet est stocké avec un chiffrement DSSE-KMS en renvoyant l'en-tête de réponse `x-amz-server-side-encryption`.

Si vous spécifiez l'en-tête `x-amz-server-side-encryption` avec une valeur de `aws:kms:dsse`, vous pouvez également utiliser les en-têtes de demandes suivants :

- `x-amz-server-side-encryption-aws-kms-key-id: SSEKMSKeyId`
- `x-amz-server-side-encryption-context: SSEKMSEncryptionContext`

Rubriques

- Opérations de l'API REST Amazon S3 prenant en charge DSSE-KMS
- Contexte de chiffrement (x-amz-server-side-encryption-context)
- AWS KMS ID de clé (x-amz-server-side-encryption-aws-kms-key-id)

Opérations de l'API REST Amazon S3 prenant en charge DSSE-KMS

Les opérations d'API REST suivantes acceptent les en-têtes de demande `x-amz-server-side-encryption`, `x-amz-server-side-encryption-aws-kms-key-id` et `x-amz-server-side-encryption-context`.

- PutObject – Lorsque vous chargez des données avec l'opération d'API PUT, vous pouvez spécifier ces en-têtes de demande.
- CopyObject – Lorsque vous copiez un objet, vous disposez d'un objet source et d'un objet cible. Lorsque vous transmettez des en-têtes DSSE-KMS avec l'opération `CopyObject`, ils s'appliquent uniquement à l'objet cible. Lorsque vous copiez un objet existant, que l'objet source soit chiffré ou non, l'objet de destination n'est pas chiffré sauf si vous demandez explicitement un chiffrement côté serveur.
- Objet POST – Lorsque vous utilisez une opération `POST` pour charger un objet, plutôt que des en-têtes de demande, vous fournissez les mêmes informations dans les champs du formulaire.
- CreateMultipartUpload – Lorsque vous chargez des objets volumineux en procédant à un chargement partitionné, vous pouvez spécifier ces en-têtes dans la demande `CreateMultipartUpload`.

Les en-têtes de réponse des opérations d'API REST suivantes renvoient l'en-tête `x-amz-server-side-encryption` lorsqu'un objet est stocké avec un chiffrement côté serveur.

- PutObject
- CopyObject
- Objet POST
- CreateMultipartUpload
- UploadPart
- UploadPartCopy
- CompleteMultipartUpload
- GetObject

- HeadObject

> **Important**
>
> - Toutes `GET` les `PUT` demandes relatives à un objet protégé par AWS KMS échouent si vous ne les créez pas à l'aide du protocole SSL (Secure Sockets Layer), du protocole TLS (Transport Layer Security) ou de la version 4 de signature.
> - Si votre objet utilise DSSE-KMS, n'envoyez pas d'en-têtes de demande de chiffrement pour les demandes `GET` et les demandes `HEAD`, car vous obtiendrez une erreur HTTP 400 (Demande incorrecte).

Contexte de chiffrement (**`x-amz-server-side-encryption-context`**)

Si vous spécifiez `x-amz-server-side-encryption:aws:kms:dsse`, l'API Simple Storage Service (Amazon S3) prend en charge un contexte de chiffrement avec l'en-tête `x-amz-server-side-encryption-context`. Un contexte de chiffrement est un ensemble de paires valeur clé qui contient des informations contextuelles supplémentaires sur les données.

Amazon S3 utilise automatiquement l'Amazon Resource Name (ARN) de l'objet en tant que paire de contexte de chiffrement ; par exemple, `arn:aws:s3:::`*`object_ARN`*.

Vous pouvez éventuellement fournir une paire de contexte de chiffrement supplémentaire à l'aide de l'en-tête `x-amz-server-side-encryption-context`. Toutefois, étant donné que le contexte de chiffrement n'est pas chiffré, assurez-vous qu'il n'inclut pas d'informations sensibles. Amazon S3 stocke cette paire de clés supplémentaire avec le contexte de chiffrement par défaut.

Pour plus d'informations sur le contexte de chiffrement dans Simple Storage Service (Amazon S3), consultez Contexte de chiffrement. Pour des informations générales sur le contexte de chiffrement, consultez la section Concepts AWS Key Management Service - Contexte de chiffrement du Guide du développeur AWS Key Management Service .

AWS KMS ID de clé (**`x-amz-server-side-encryption-aws-kms-key-id`**)

Vous pouvez utiliser l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` pour spécifier l'ID de la clé gérée par le client utilisée pour protéger les données. Si vous spécifiez l'`x-amz-server-side-encryption:aws:kms:dsse`en-tête mais que vous ne le `x-amz-server-`

`side-encryption-aws-kms-key-id` fournissez pas, Amazon S3 utilise le Clé gérée par AWS (`aws/s3`) pour protéger les données. Si vous souhaitez utiliser une clé gérée par le client, vous devrez fournir l'en-tête `x-amz-server-side-encryption-aws-kms-key-id` de la clé gérée par le client.

> **Important**
>
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 ne prend en charge que les clés KMS à chiffrement symétrique. Pour plus d'informations sur ces clés, consultez Clés KMS de chiffrement symétriques dans le Guide du développeur AWS Key Management Service .

À l'aide du AWS CLI

Lorsque vous chargez un nouvel objet ou copiez un objet existant, vous pouvez spécifier l'utilisation de DSSE-KMS pour chiffrer vos données. Pour ce faire, ajoutez le paramètre `--server-side-encryption aws:kms:dsse` à l'en-tête. Utilisez le paramètre `--ssekms-key-id` *`example-key-id`* pour ajouter la clé AWS KMS gérée par le client que vous avez créée. Si vous spécifiez`--server-side-encryption aws:kms:dsse`, mais que vous ne fournissez pas d'identifiant de AWS KMS clé, Amazon S3 utilisera la clé AWS gérée (`aws/s3`).

```
aws s3api put-object --bucket amzn-s3-demo-bucket --key example-object-key --server-side-encryption aws:kms:dsse --ssekms-key-id example-key-id --body filepath
```

Vous pouvez chiffrer un objet non chiffré pour utiliser DSSE-KMS en recopiant l'objet à son emplacement.

```
aws s3api copy-object --bucket amzn-s3-demo-bucket --key example-object-key --copy-source amzn-s3-demo-bucket/example-object-key --server-side-encryption aws:kms:dsse --ssekms-key-id example-key-id
```

Utilisation du chiffrement côté serveur avec les clés fournies par le client (SSE-C)

Le chiffrement côté serveur consiste à protéger les données au repos. Un chiffrement côté serveur chiffre uniquement les données d'objet, pas les métadonnées d'objet. Dans le cadre du chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C), vous pouvez stocker

vos données chiffrées avec vos propres clés de chiffrement. Avec la clé de chiffrement que vous fournissez dans la demande, Amazon S3 gère le chiffrement des données quand il écrit sur les disques et le déchiffrement des données quand vous accédez à vos objets. Par conséquent, vous n'avez pas besoin de conserver de code pour procéder au chiffrement et déchiffrement des données. Il ne vous reste qu'à gérer les clés de chiffrement que vous fournissez.

Quand vous chargez un objet, Amazon S3 utilise la clé de chiffrement que vous fournissez pour appliquer le chiffrement AES-256 à vos données. Amazon S3 supprime ensuite la clé de chiffrement de la mémoire. Lorsque vous récupérez un objet, vous devez fournir la même clé de chiffrement dans la demande. Amazon S3 vérifie tout d'abord que la clé de chiffrement que vous avez fournie correspond, puis il déchiffre l'objet avant de vous renvoyer les données de ce dernier.

Aucuns frais supplémentaires ne s'appliquent à l'utilisation du chiffrement SSE-C. Toutefois, les demandes de configuration et d'utilisation du chiffrement SSE-C entraînent des frais de demande Amazon S3 standard. Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3.

> **Note**
>
> Amazon S3 ne stocke pas la clé de chiffrement que vous fournissez. À la place, il stocke un code d'authentification de message utilisant hash (HMAC) crypté de manière aléatoire de la clé de chiffrement pour valider les demandes futures. La valeur HMAC cryptée ne peut pas être utilisée pour retrouver la valeur de la clé de chiffrement ou pour déchiffrer les contenus de l'objet chiffré. Cela signifie que si vous perdez la clé de chiffrement, vous perdez l'objet.

S3 Replication prend en charge les objets chiffrés avec le SSE-C. Pour plus d'informations sur la réplication des objets chiffrés, consultez the section called "Réplication d'objets chiffrés".

Pour plus d'informations sur SSE-C, consultez les rubriques suivantes :

Rubriques

- Présentation des SSE-C
- Exigence et restriction des SSE-C
- Présigné URLs et SSE-C
- Spécification du chiffrement côté serveur avec des clés fournies par le client (SSE-C)

Présentation des SSE-C

Cette section fournit une présentation du chiffrement SSE-C. Dans le cadre du chiffrement SSE-C, gardez à l'esprit les considérations suivantes.

- Vous devez utiliser HTTPS.

> **Important**
>
> Amazon S3 rejette toute demande faite via HTTP lors de l'utilisation du chiffrement SSE-C. Pour des raisons de sécurité, nous vous recommandons de considérer toute clé que vous envoyez par erreur via HTTP comme compromise. Écartez la clé et permutez comme il convient.

- L'étiquette d'entité (ETag) dans la réponse n'est pas le MD5 hachage des données de l'objet.
- Vous gérez un mappage pour savoir quelle clé de chiffrement a été utilisée pour chiffrer quel objet. Amazon S3 ne stocke pas les clés de chiffrement. Vous devez assurer le suivi pour savoir quelle clé de chiffrement a été fournie pour quel objet.
  - Si votre compartiment prend en charge la gestion des versions, chaque version d'objet que vous chargez à l'aide de cette fonctionnalité peut avoir sa propre clé de chiffrement. Vous devez assurer le suivi pour savoir quelle clé de chiffrement a été utilisée pour quelle version d'objet.
  - Etant donné que vous gérez les clés de chiffrement du côté client, vous gérez toute sauvegarde supplémentaire, comme la rotation des clés, du côté client.

> **Warning**
>
> Si vous perdez la clé de chiffrement, toute requête `GET` d'un objet sans clé de chiffrement échoue et vous perdez l'objet.

Exigence et restriction des SSE-C

Pour exiger le chiffrement SSE-C de tous les objets figurant dans un compartiment Amazon S3 particulier, vous pouvez utiliser une politique de compartiment.

Par exemple, la politique de compartiment suivante refuse les autorisations de chargement d'objet (`s3:PutObject`) autorisations pour toutes les demandes qui n'incluent pas l'en-tête `x-amz-server-side-encryption-customer-algorithm` demandant SSE-C.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RequireSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "true"
                }
            }
        }
    ]
}
```

Vous pouvez également utiliser une politique pour limiter le chiffrement côté serveur de tous les objets figurant dans un compartiment Amazon S3 particulier. Par exemple, la politique de compartiment suivante n'autorise pas le chargement d'objet (`s3:PutObject`) si la demande inclut l'en-tête `x-amz-server-side-encryption-customer-algorithm` demandant le chiffrement SSE-C.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "PutObjectPolicy",
    "Statement": [
        {
            "Sid": "RestrictSSECObjectUploads",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
```

```
            "Condition": {
                "Null": {
                    "s3:x-amz-server-side-encryption-customer-algorithm": "false"
                }
            }
        }
    ]
}
```

> **Important**
>
> Si vous utilisez une politique de compartiment pour activer SSE-C`s3:PutObject`, vous devez inclure l'`x-amz-server-side-encryption-customer-algorithm`en-tête dans toutes les demandes de téléchargement partitionné (CreateMultipartUpload UploadPart, et). CompleteMultipartUpload

Présigné URLs et SSE-C

Vous pouvez générer une URL pré-signée qui peut être utilisée pour des opérations comme le chargement d'un nouvel objet, la récupération d'un objet existant ou la récupération des métadonnées d'objet. URLsSupporte le SSE-C présigné comme suit :

- Lors de la création d'une URL pré-signée, vous devez spécifier l'algorithme en utilisant l'en-tête `x-amz-server-side-encryption-customer-algorithm` dans le calcul de la signature.
- Lorsque vous utilisez l'URL pré-signée pour charger un nouvel objet, récupérer un objet existant ou récupérer uniquement des métadonnées d'objet, vous devez fournir tous les en-têtes de chiffrement dans la demande de votre application cliente.

> **Note**
>
> Pour les non-SSE-C objets, vous pouvez générer une URL présignée et coller directement cette URL dans un navigateur pour accéder aux données.
> Toutefois, vous ne pouvez pas procéder ainsi pour des objets SSE-C, car en plus de l'URL pré-signée, vous devez également inclure des en-têtes HTTP spécifiques aux objets SSE-C. Par conséquent, vous ne pouvez utiliser le présigné URLs pour les objets SSE-C que par programmation.

Pour plus d'informations sur le présigné URLs, consultezthe section called “Utilisation du présigné URLs pour télécharger et charger des objets”.

Spécification du chiffrement côté serveur avec des clés fournies par le client (SSE-C)

Au moment de la création de l'objet avec l'API REST, vous pouvez spécifier un chiffrement côté serveur avec les clés fournies par le client (SSE-C). Lorsque vous utilisez SSE-C, vous devez fournir des informations de clé de chiffrement à l'aide des en-têtes de demande suivants.

Nom	Description
`x-amz-server-side-encryption-customer-algorithm`	Utilisez cet en-tête pour spécifier l'algorithme du chiffrement. La valeur de l'en-tête doit être `AES256`.
`x-amz-server-side-encryption-customer-key`	Utilisez cet en-tête pour fournir la clé de chiffrement de 256 bits encodée en Base64 qu'Amazon S3 doit utiliser pour chiffrer ou déchiffrer les données.
`x-amz-server-side-encryption-customer-key-MD5`	Utilisez cet en-tête pour fournir le MD5 résumé de 128 bits codé en base64 de la clé de chiffrement conformément à la RFC 1321. Amazon S3 utilise cet en-tête pour vérifier l'intégrité du message et veiller à ce que la clé de chiffrement ait été transmise sans erreur.

Vous pouvez utiliser les bibliothèques d'encapsulation du AWS SDK pour ajouter ces en-têtes à votre demande. Si nécessaire, vous pouvez effectuer les appels à l'API REST Amazon S3 directement dans l'application.

> **Note**
>
> Vous ne pouvez pas utiliser la console Amazon S3 pour charger un objet et demander des clés SSE-C. Vous ne pouvez pas non plus utiliser la console pour mettre à jour (par exemple, modifier la classe de stockage ou ajouter des métadonnées) un objet existant stocké à l'aide de clés SSE-C.

Utilisation de l'API REST

Repos Amazon S3 APIs compatible SSE-C

Les Amazon S3 suivants prennent en APIs charge le chiffrement côté serveur à l'aide de clés de chiffrement fournies par le client (SSE-C).

- Opération GET – Lorsque vous récupérez des objets via l'API GET (consultez GET Object), vous pouvez spécifier ces en-têtes de demande.
- Opération HEAD – Pour récupérer les métadonnées d'objet via l'API HEAD (consultez Head Object), vous pouvez spécifier ces en-têtes de demande.
- Opération PUT – Lorsque vous chargez des données via l'API PutObject (consultez PutObject), vous pouvez spécifier ces en-têtes de demande.
- Chargement partitionné – Lorsque vous chargez des objets volumineux via l'API de chargement partitionné, vous pouvez spécifier ces en-têtes. Vous spécifiez ces en-têtes dans la demande initiale (consultez Lancement du chargement partitionné (langue française non garantie)) et dans chaque demande de chargement de partie suivante (consultez Chargement d'une partie ou Chargement d'une partie (Copy) (langue française non garantie)). Pour chaque demande de chargement d'une partie, les informations de chiffrement doivent être les mêmes que celles fournies dans la demande de lancement du chargement partitionné.
- Opération POST – Lorsque vous utilisez une opération POST pour charger un objet (consultez POST Object), à la place des en-têtes de demande, fournissez les mêmes informations dans les champs du formulaire.
- Opération Copy – Lorsque vous copiez un objet (consultez PUT Object - Copy), vous disposez d'un objet source et d'un objet cible :
  - Si vous souhaitez que l'objet cible soit chiffré à l'aide du chiffrement côté serveur avec des clés AWS gérées, vous devez fournir l'en-tête de `x-amz-server-side-encryption` demande.
  - Si vous souhaitez chiffrer l'objet cible grâce aux SSE-C, vous devez fournir des informations de chiffrement grâce aux trois en-têtes décrits dans le tableau précédent.
  - Si l'objet source est chiffré grâce aux SSE-C, vous devez fournir les informations sur la clé de chiffrement grâce aux en-têtes suivants afin qu'Amazon S3 puisse déchiffrer l'objet pour le copier.

Nom	Description
`x-amz-copy-source-server-side-encryption-customer-algorithm`	Incluez cet en-tête pour spécifier l'algorithme qu'Amazon S3 doit utiliser pour déchiffrer l'objet source. La valeur doit être `AES256`.
`x-amz-copy-source-server-side-encryption-customer-key`	Incluez cet en-tête pour fournir la clé de chiffrement encodée en Base64 qu'Amazon S3 doit utiliser pour déchiffrer l'objet source. La clé de chiffrement doit être celle fournie à Amazon S3 lorsque vous avez créé l'objet source. Sinon, Amazon S3 ne peut pas déchiffrer l'objet.
`x-amz-copy-source-server-side-encryption-customer-key-MD5`	Incluez cet en-tête pour fournir le MD5 résumé de 128 bits codé en base64 de la clé de chiffrement conformément à la RFC 1321.

Utilisation du AWS SDKs pour spécifier le SSE-C pour les opérations PUT, GET, Head et Copy

Les exemples suivants illustrent la demande d'un chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C) pour les objets. Les exemples exécutent les opérations suivantes. Chaque opération montre comment spécifier SSE-C-related les en-têtes dans la demande :

- Put object – Charge un objet et demande un chiffrement côté serveur avec une clé de chiffrement fournie par le client.
- Get object – Télécharge l'objet chargé à l'étape précédente. Dans la demande, vous fournissez les mêmes informations de chiffrement que celles fournies lors du chargement de l'objet. Amazon S3 a besoin de ces informations pour déchiffrer l'objet afin de pouvoir vous le renvoyer.
- Get object metadata – Récupère les métadonnées de l'objet. Vous fournissez les mêmes informations de chiffrement que celles utilisées quand l'objet a été chargé.

- Copy object – Effectue une copie de l'objet précédemment chargé. Comme l'objet source est stocké via SSE-C, vous devez fournir ses informations de chiffrement dans votre demande de copie. Par défaut, Amazon S3 ne chiffre la copie de l'objet que si vous le demandez explicitement. Cet exemple demande à Amazon S3 de stocker une copie chiffrée de l'objet.

Java

> **Note**
>
> Cet exemple montre comment copier un objet en une seule opération. Lorsque vous utilisez l'API de chargement partitionné pour charger des objets volumineux, vous fournissez les informations de chiffrement comme illustré dans l'exemple suivant. Pour des exemples de téléchargements partitionnés utilisant le AWS SDK pour Java, voir. Chargement d'un objet à l'aide du chargement partitionné

Pour ajouter les informations de chiffrement requises, vous incluez une clé `SSECustomerKey` dans votre demande. Pour plus d'informations sur la classe `SSECustomerKey`, consultez la section API REST.

Pour plus d'informations sur SSE-C, consultez Utilisation du chiffrement côté serveur avec les clés fournies par le client (SSE-C). Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import javax.crypto.KeyGenerator;
import java.io.BufferedReader;
import java.io.File;
import java.io.IOException;
import java.io.InputStreamReader;
```

```
import java.security.NoSuchAlgorithmException;
import java.security.SecureRandom;

public class ServerSideEncryptionUsingClientSideEncryptionKey {
    private static SSECustomerKey SSE_KEY;
    private static AmazonS3 S3_CLIENT;
    private static KeyGenerator KEY_GENERATOR;

    public static void main(String[] args) throws IOException,
 NoSuchAlgorithmException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String keyName = "*** Key name ***";
        String uploadFileName = "*** File path ***";
        String targetKeyName = "*** Target key name ***";

        // Create an encryption key.
        KEY_GENERATOR = KeyGenerator.getInstance("AES");
        KEY_GENERATOR.init(256, new SecureRandom());
        SSE_KEY = new SSECustomerKey(KEY_GENERATOR.generateKey());

        try {
            S3_CLIENT = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Upload an object.
            uploadObject(bucketName, keyName, new File(uploadFileName));

            // Download the object.
            downloadObject(bucketName, keyName);

            // Verify that the object is properly encrypted by attempting to
 retrieve it
            // using the encryption key.
            retrieveObjectMetadata(bucketName, keyName);

            // Copy the object into a new object that also uses SSE-C.
            copyObject(bucketName, keyName, targetKeyName);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
```

```
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void uploadObject(String bucketName, String keyName, File file) {
        PutObjectRequest putRequest = new PutObjectRequest(bucketName, keyName,
file).withSSECustomerKey(SSE_KEY);
        S3_CLIENT.putObject(putRequest);
        System.out.println("Object uploaded");
    }

    private static void downloadObject(String bucketName, String keyName) throws
IOException {
        GetObjectRequest getObjectRequest = new GetObjectRequest(bucketName,
keyName).withSSECustomerKey(SSE_KEY);
        S3Object object = S3_CLIENT.getObject(getObjectRequest);

        System.out.println("Object content: ");
        displayTextInputStream(object.getObjectContent());
    }

    private static void retrieveObjectMetadata(String bucketName, String keyName) {
        GetObjectMetadataRequest getMetadataRequest = new
GetObjectMetadataRequest(bucketName, keyName)
                .withSSECustomerKey(SSE_KEY);
        ObjectMetadata objectMetadata =
S3_CLIENT.getObjectMetadata(getMetadataRequest);
        System.out.println("Metadata retrieved. Object size: " +
objectMetadata.getContentLength());
    }

    private static void copyObject(String bucketName, String keyName, String
targetKeyName)
            throws NoSuchAlgorithmException {
        // Create a new encryption key for target so that the target is saved using
        // SSE-C.
        SSECustomerKey newSSEKey = new SSECustomerKey(KEY_GENERATOR.generateKey());

        CopyObjectRequest copyRequest = new CopyObjectRequest(bucketName, keyName,
bucketName, targetKeyName)
                .withSourceSSECustomerKey(SSE_KEY)
```

```
                .withDestinationSSECustomerKey(newSSEKey);

        S3_CLIENT.copyObject(copyRequest);
        System.out.println("Object copied");
    }

    private static void displayTextInputStream(S3ObjectInputStream input) throws
 IOException {
        // Read one line at a time from the input stream and display each line.
        BufferedReader reader = new BufferedReader(new InputStreamReader(input));
        String line;
        while ((line = reader.readLine()) != null) {
            System.out.println(line);
        }
        System.out.println();
    }
}
```

.NET

> **Note**
>
> Pour obtenir des exemples de chargement d'objets volumineux à l'aide de l'API de chargement partitionné, consultez Chargement d'un objet à l'aide du chargement partitionné et Utilisation de AWS SDKs (API de bas niveau).

Pour plus d'informations sur SSE-C, consultez Utilisation du chiffrement côté serveur avec les clés fournies par le client (SSE-C). Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;
```

```
namespace Amazon.DocSamples.S3
{
    class SSEClientEncryptionKeyObjectOperationsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string keyName = "*** key name for new object created ***";
        private const string copyTargetKeyName = "*** key name for object copy ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            ObjectOpsUsingClientEncryptionKeyAsync().Wait();
        }
        private static async Task ObjectOpsUsingClientEncryptionKeyAsync()
        {
            try
            {
                // Create an encryption key.
                Aes aesEncryption = Aes.Create();
                aesEncryption.KeySize = 256;
                aesEncryption.GenerateKey();
                string base64Key = Convert.ToBase64String(aesEncryption.Key);

                // 1. Upload the object.
                PutObjectRequest putObjectRequest = await
 UploadObjectAsync(base64Key);
                // 2. Download the object and verify that its contents matches what
 you uploaded.
                await DownloadObjectAsync(base64Key, putObjectRequest);
                // 3. Get object metadata and verify that the object uses AES-256
 encryption.
                await GetObjectMetadataAsync(base64Key);
                // 4. Copy both the source and target objects using server-side
 encryption with
                //    a customer-provided encryption key.
                await CopyObjectAsync(aesEncryption, base64Key);
            }
            catch (AmazonS3Exception e)
            {
```

```
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        private static async Task<PutObjectRequest> UploadObjectAsync(string
base64Key)
        {
            PutObjectRequest putObjectRequest = new PutObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                ContentBody = "sample text",
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };
            PutObjectResponse putObjectResponse = await
client.PutObjectAsync(putObjectRequest);
            return putObjectRequest;
        }
        private static async Task DownloadObjectAsync(string base64Key,
PutObjectRequest putObjectRequest)
        {
            GetObjectRequest getObjectRequest = new GetObjectRequest
            {
                BucketName = bucketName,
                Key = keyName,
                // Provide encryption information for the object stored in Amazon
S3.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            using (GetObjectResponse getResponse = await
client.GetObjectAsync(getObjectRequest))
            using (StreamReader reader = new
StreamReader(getResponse.ResponseStream))
```

```
            {
                string content = reader.ReadToEnd();
                if (String.Compare(putObjectRequest.ContentBody, content) == 0)
                    Console.WriteLine("Object content is same as we uploaded");
                else
                    Console.WriteLine("Error...Object content is not same.");

                if (getResponse.ServerSideEncryptionCustomerMethod ==
ServerSideEncryptionCustomerMethod.AES256)
                    Console.WriteLine("Object encryption method is AES256, same as
we set");
                else
                    Console.WriteLine("Error...Object encryption method is not the
same as AES256 we set");

                // Assert.AreEqual(putObjectRequest.ContentBody, content);
                // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getResponse.ServerSideEncryptionCustomerMethod);
            }
        }
        private static async Task GetObjectMetadataAsync(string base64Key)
        {
            GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest
            {
                BucketName = bucketName,
                Key = keyName,

                // The object stored in Amazon S3 is encrypted, so provide the
necessary encryption information.
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            GetObjectMetadataResponse getObjectMetadataResponse = await
client.GetObjectMetadataAsync(getObjectMetadataRequest);
            Console.WriteLine("The object metadata show encryption method used is:
{0}", getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
            // Assert.AreEqual(ServerSideEncryptionCustomerMethod.AES256,
getObjectMetadataResponse.ServerSideEncryptionCustomerMethod);
        }
        private static async Task CopyObjectAsync(Aes aesEncryption, string
base64Key)
```

```
        {
            aesEncryption.GenerateKey();
            string copyBase64Key = Convert.ToBase64String(aesEncryption.Key);

            CopyObjectRequest copyRequest = new CopyObjectRequest
            {
                SourceBucket = bucketName,
                SourceKey = keyName,
                DestinationBucket = bucketName,
                DestinationKey = copyTargetKeyName,
                // Information about the source object's encryption.
                CopySourceServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
                CopySourceServerSideEncryptionCustomerProvidedKey = base64Key,
                // Information about the target object's encryption.
                ServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = copyBase64Key
            };
            await client.CopyObjectAsync(copyRequest);
        }
    }
}
```

Utilisation du AWS SDKs pour spécifier le SSE-C pour les téléchargements partitionnés

L'exemple de la section précédente montre comment demander le chiffrement côté serveur à l'aide d'une clé de chiffrement fournie par le client (SSE-C) dans les opérations PUT, GET, Head et Copy. Cette section décrit les autres Amazon S3 APIs qui prennent en charge le SSE-C.

Java

Pour charger des objets volumineux, vous pouvez utiliser l'API de chargement partitionné (consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3). Vous pouvez utiliser le haut niveau ou le bas niveau APIs pour télécharger des objets de grande taille. Ils APIs prennent en charge les en-têtes liés au chiffrement dans la demande.

- Lorsque vous utilisez l'API `TransferManager` de haut niveau, vous fournissez les en-têtes propres au chiffrement dans l'objet `PutObjectRequest` (voir Chargement d'un objet à l'aide du chargement partitionné).

- Lorsque vous utilisez l'API de bas niveau, vous fournissez les informations de chiffrement dans l'objet `InitiateMultipartUploadRequest`, suivies des mêmes informations dans chaque `UploadPartRequest`. Il est inutile de fournir des en-têtes liés au chiffrement dans votre objet `CompleteMultipartUploadRequest`. Pour obtenir des exemples, consultez Utilisation de AWS SDKs (API de bas niveau).

L'exemple ci-dessous utilise `TransferManager` pour créer des objets ; il explique également la marche à suivre pour fournir des informations SSE-C. Cet exemple effectue les opérations suivantes :

- Crée un objet à l'aide de la méthode `TransferManager.upload()`. Dans l'instance `PutObjectRequest`, vous fournissez à la demande les informations de clé de chiffrement. Amazon S3 chiffre l'objet en utilisant la clé fournie par le client.
- Effectue une copie de l'objet en appelant la méthode `TransferManager.copy()`. L'exemple demande à Amazon S3 de chiffrer la copie de l'objet à l'aide d'un nouvel objet `SSECustomerKey`. L'objet source étant chiffré au moyen de SSE-C, `CopyObjectRequest`fournit également la clé de chiffrement de l'objet source, afin qu'Amazon S3 puisse déchiffrer l'objet avant de le copier.

Example

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;
import com.amazonaws.services.s3.model.PutObjectRequest;
import com.amazonaws.services.s3.model.SSECustomerKey;
import com.amazonaws.services.s3.transfer.Copy;
import com.amazonaws.services.s3.transfer.TransferManager;
import com.amazonaws.services.s3.transfer.TransferManagerBuilder;
import com.amazonaws.services.s3.transfer.Upload;

import javax.crypto.KeyGenerator;
import java.io.File;
import java.security.SecureRandom;
```

```
public class ServerSideEncryptionCopyObjectUsingHLwithSSEC {

    public static void main(String[] args) throws Exception {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";
        String fileToUpload = "*** File path ***";
        String keyName = "*** New object key name ***";
        String targetKeyName = "*** Key name for object copy ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withRegion(clientRegion)
                    .withCredentials(new ProfileCredentialsProvider())
                    .build();
            TransferManager tm = TransferManagerBuilder.standard()
                    .withS3Client(s3Client)
                    .build();

            // Create an object from a file.
            PutObjectRequest putObjectRequest = new PutObjectRequest(bucketName,
 keyName, new File(fileToUpload));

            // Create an encryption key.
            KeyGenerator keyGenerator = KeyGenerator.getInstance("AES");
            keyGenerator.init(256, new SecureRandom());
            SSECustomerKey sseCustomerEncryptionKey = new
 SSECustomerKey(keyGenerator.generateKey());

            // Upload the object. TransferManager uploads asynchronously, so this
 call
            // returns immediately.
            putObjectRequest.setSSECustomerKey(sseCustomerEncryptionKey);
            Upload upload = tm.upload(putObjectRequest);

            // Optionally, wait for the upload to finish before continuing.
            upload.waitForCompletion();
            System.out.println("Object created.");

            // Copy the object and store the copy using SSE-C with a new key.
            CopyObjectRequest copyObjectRequest = new CopyObjectRequest(bucketName,
 keyName, bucketName, targetKeyName);
            SSECustomerKey sseTargetObjectEncryptionKey = new
 SSECustomerKey(keyGenerator.generateKey());
```

```
            copyObjectRequest.setSourceSSECustomerKey(sseCustomerEncryptionKey);

 copyObjectRequest.setDestinationSSECustomerKey(sseTargetObjectEncryptionKey);

            // Copy the object. TransferManager copies asynchronously, so this call
 returns
            // immediately.
            Copy copy = tm.copy(copyObjectRequest);

            // Optionally, wait for the upload to finish before continuing.
            copy.waitForCompletion();
            System.out.println("Copy complete.");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Pour télécharger des objets volumineux, vous pouvez utiliser l'API de téléchargement partitionné (voirChargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3). AWS Le SDK pour .NET fournit des fonctionnalités de haut niveau ou de APIs bas niveau pour le téléchargement d'objets volumineux. Ils APIs prennent en charge les en-têtes liés au chiffrement dans la demande.

- Lorsque vous utilisez l'API de haut niveau `Transfer-Utility` , vous fournissez les en-têtes propres au chiffrement dans l'objet `TransferUtilityUploadRequest` comme illustré. Pour des exemples de code, consultez Chargement d'un objet à l'aide du chargement partitionné.

```
TransferUtilityUploadRequest request = new TransferUtilityUploadRequest()
{
    FilePath = filePath,
    BucketName = existingBucketName,
    Key = keyName,
```

```
    // Provide encryption information.
    ServerSideEncryptionCustomerMethod =
 ServerSideEncryptionCustomerMethod.AES256,
    ServerSideEncryptionCustomerProvidedKey = base64Key,
};
```

- Lorsque vous utilisez l'API de bas niveau, vous fournissez des informations de chiffrement dans votre demande de lancement du chargement partitionné. Ces informations de chiffrement doivent être identiques dans les demandes de chargement partitionné qui suivent. Il est toutefois inutile de fournir des en-têtes liés au chiffrement dans votre demande de fin de chargement partitionné. Pour obtenir des exemples, consultez Utilisation de AWS SDKs (API de bas niveau).

  L'exemple suivant concerne un chargement partitionné de niveau inférieur exécutant une copie d'un objet volumineux existant. Dans cet exemple, l'objet à copier est stocké dans Amazon S3 à l'aide d'une clé SSE-C, et vous souhaitez également enregistrer l'objet cible à l'aide d'une clé SSE-C. Dans l'exemple, vous procédez comme suit :

  - Initier une demande de chargement partitionné en fournissant une clé de chiffrement et les informations connexes.
  - Fournir les clés de chiffrement de l'objet source et cible et les informations relatives dans la `CopyPartRequest`.
  - Obtenir la taille de l'objet source à copier en récupérant les métadonnées de l'objet.
  - Charger les objets par lots de 5 Mo.

  Example

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.IO;
using System.Security.Cryptography;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class SSECLowLevelMPUcopyObjectTest
    {
        private const string existingBucketName = "*** bucket name ***";
```

```
        private const string sourceKeyName      = "*** source object key name
***";
        private const string targetKeyName      = "*** key name for the target
object ***";
        private const string filePath           = @"*** file path ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CopyObjClientEncryptionKeyAsync().Wait();
        }

        private static async Task CopyObjClientEncryptionKeyAsync()
        {
            Aes aesEncryption = Aes.Create();
            aesEncryption.KeySize = 256;
            aesEncryption.GenerateKey();
            string base64Key = Convert.ToBase64String(aesEncryption.Key);

            await CreateSampleObjUsingClientEncryptionKeyAsync(base64Key,
s3Client);

            await CopyObjectAsync(s3Client, base64Key);
        }
        private static async Task CopyObjectAsync(IAmazonS3 s3Client, string
base64Key)
        {
            List<CopyPartResponse> uploadResponses = new List<CopyPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = targetKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key,
            };

            InitiateMultipartUploadResponse initResponse =
```

```
                await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB
            long firstByte = 0;
            long lastByte = partSize;

            try
            {
                // First find source object size. Because object is stored
encrypted with
                // customer provided key you need to provide encryption
information in your request.
                GetObjectMetadataRequest getObjectMetadataRequest = new
GetObjectMetadataRequest()
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                    ServerSideEncryptionCustomerProvidedKey = base64Key // " *
**source object encryption key ***"
                };

                GetObjectMetadataResponse getObjectMetadataResponse = await
s3Client.GetObjectMetadataAsync(getObjectMetadataRequest);

                long filePosition = 0;
                for (int i = 1; filePosition <
getObjectMetadataResponse.ContentLength; i++)
                {
                    CopyPartRequest copyPartRequest = new CopyPartRequest
                    {
                        UploadId = initResponse.UploadId,
                        // Source.
                        SourceBucket = existingBucketName,
                        SourceKey = sourceKeyName,
                        // Source object is stored using SSE-C. Provide encryption
information.
                        CopySourceServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        CopySourceServerSideEncryptionCustomerProvidedKey =
base64Key, //"***source object encryption key ***",
                        FirstByte = firstByte,
```

```
                        // If the last part is smaller then our normal part size
then use the remaining size.
                        LastByte = lastByte >
getObjectMetadataResponse.ContentLength ?
                            getObjectMetadataResponse.ContentLength - 1 :
lastByte,

                        // Target.
                        DestinationBucket = existingBucketName,
                        DestinationKey = targetKeyName,
                        PartNumber = i,
                        // Encryption information for the target object.
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };
                    uploadResponses.Add(await
s3Client.CopyPartAsync(copyPartRequest));
                    filePosition += partSize;
                    firstByte += partSize;
                    lastByte += partSize;
                }

                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
                    UploadId = initResponse.UploadId,
                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);
            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = targetKeyName,
```

```
                    UploadId = initResponse.UploadId
                };
                s3Client.AbortMultipartUpload(abortMPURequest);
            }
        }
        private static async Task
CreateSampleObjUsingClientEncryptionKeyAsync(string base64Key, IAmazonS3
s3Client)
        {
            // List to store upload part responses.
            List<UploadPartResponse> uploadResponses = new
List<UploadPartResponse>();

            // 1. Initialize.
            InitiateMultipartUploadRequest initiateRequest = new
InitiateMultipartUploadRequest
            {
                BucketName = existingBucketName,
                Key = sourceKeyName,
                ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                ServerSideEncryptionCustomerProvidedKey = base64Key
            };

            InitiateMultipartUploadResponse initResponse =
               await s3Client.InitiateMultipartUploadAsync(initiateRequest);

            // 2. Upload Parts.
            long contentLength = new FileInfo(filePath).Length;
            long partSize = 5 * (long)Math.Pow(2, 20); // 5 MB

            try
            {
                long filePosition = 0;
                for (int i = 1; filePosition < contentLength; i++)
                {
                    UploadPartRequest uploadRequest = new UploadPartRequest
                    {
                        BucketName = existingBucketName,
                        Key = sourceKeyName,
                        UploadId = initResponse.UploadId,
                        PartNumber = i,
                        PartSize = partSize,
                        FilePosition = filePosition,
```

```
                        FilePath = filePath,
                        ServerSideEncryptionCustomerMethod =
ServerSideEncryptionCustomerMethod.AES256,
                        ServerSideEncryptionCustomerProvidedKey = base64Key
                    };

                    // Upload part and add response to our list.
                    uploadResponses.Add(await
s3Client.UploadPartAsync(uploadRequest));

                    filePosition += partSize;
                }

                // Step 3: complete.
                CompleteMultipartUploadRequest completeRequest = new
CompleteMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId,
                    //PartETags = new List<PartETag>(uploadResponses)

                };
                completeRequest.AddPartETags(uploadResponses);

                CompleteMultipartUploadResponse completeUploadResponse =
                    await s3Client.CompleteMultipartUploadAsync(completeRequest);

            }
            catch (Exception exception)
            {
                Console.WriteLine("Exception occurred: {0}", exception.Message);
                AbortMultipartUploadRequest abortMPURequest = new
AbortMultipartUploadRequest
                {
                    BucketName = existingBucketName,
                    Key = sourceKeyName,
                    UploadId = initResponse.UploadId
                };
                await s3Client.AbortMultipartUploadAsync(abortMPURequest);
            }
        }
    }
```

```
}
```

Protection des données avec le chiffrement côté client

Le chiffrement côté client est le fait de chiffrer vos données localement pour garantir leur sécurité en transit et au repos. Pour chiffrer vos objets avant de les envoyer à Amazon S3, utilisez le client de chiffrement Amazon S3. Lorsque vos objets sont chiffrés de cette manière, ils ne sont exposés à aucun tiers, y compris AWS. Amazon S3 reçoit vos objets déjà chiffrés. Amazon S3 ne joue aucun rôle dans le chiffrement ou le déchiffrement de vos objets. Vous pouvez utiliser à la fois le client de chiffrement Amazon 3 et le chiffrement côté serveur pour chiffrer vos données. Lorsque vous envoyez des objets chiffrés à Amazon S3, Amazon S3 ne reconnaît pas les objets comme étant chiffrés, il ne détecte que des objets classiques.

Le client de chiffrement Amazon S3 fait office d'intermédiaire entre vous et Amazon S3. Une fois que vous avez instancié le client de chiffrement Amazon S3, vos objets sont automatiquement chiffrés et déchiffrés dans le cadre de vos demandes Amazon S3 `PutObject` et `GetObject`. Vos objets sont tous chiffrés à l'aide d'une clé de données unique. Le client de chiffrement Amazon S3 n'utilise ni n'interagit avec les clés de compartiment, même si vous spécifiez une clé KMS comme clé d'encapsulation.

Le Manuel du développeur du client de chiffrement Amazon S3 se concentre sur les versions 3.0 et ultérieures du client de chiffrement Amazon S3. Pour plus d'informations, consultez What is the Amazon S3 Encryption Client? (Qu'est-ce que le client de chiffrement Amazon S3) dans le Guide du développeur du client de chiffrement Amazon S3.

Pour plus d'informations sur les versions précédentes du client Amazon S3 Encryption, consultez le guide du développeur du AWS SDK correspondant à votre langage de programmation.

- AWS SDK pour Java
- AWS SDK pour .NET
- AWS SDK pour Go
- AWS SDK pour PHP
- AWS SDK pour Ruby
- AWS SDK pour C++

Confidentialité du trafic inter-réseau

Cette rubrique décrit comment Amazon S3 sécurise les connexions depuis le service vers d'autres emplacements.

Trafic entre les clients de service et sur site et les applications

Les connexions suivantes peuvent être combinées AWS PrivateLink pour fournir une connectivité entre votre réseau privé et AWS :

- Une connexion AWS Site-to-Site VPN. Pour plus d'informations, voir Qu'est-ce que c'est AWS Site-to-Site VPN ?
- Une AWS Direct Connect connexion. Pour plus d'informations, voir Qu'est-ce que c'est AWS Direct Connect ?

L'accès à Amazon S3 via le réseau se fait via la AWS publication APIs. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2. Nous recommandons TLS 1.3. Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes. De plus, vous devez signer les demandes à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète, associées à un principal IAM. Vous pouvez également utiliser le service AWS Security Token Service (STS) afin de générer des informations d'identification de sécurité temporaires pour signer les demandes.

Trafic entre les AWS ressources d'une même région

Un point de terminaison de VPC (Virtual Private Cloud) pour Amazon S3 est une entité logique au sein d'un VPC qui autorise la connectivité uniquement à Amazon S3. Le VPC achemine les demandes vers Amazon S3 et les réponses en retour vers le VPC. Pour plus d'informations, consultez Points de terminaison d'un VPC dans le Guide de l'utilisateur de VPC. Pour obtenir des exemples de politique de compartiment que vous pouvez utiliser pour contrôler l'accès aux compartiments S3 à partir de points de terminaison d'un VPC, consultez Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment.

AWS PrivateLink pour Amazon S3

Avec AWS PrivateLink Amazon S3, vous pouvez provisionner des points de terminaison VPC d'interface (points de terminaison d'interface) dans votre cloud privé virtuel (VPC). Ces points de terminaison sont directement accessibles depuis des applications installées sur site via VPN et/ou via un autre Région AWS système de peering VPC. AWS Direct Connect

Les points de terminaison d'interface sont représentés par une ou plusieurs interfaces réseau élastiques (ENIs) auxquelles sont attribuées des adresses IP privées provenant de sous-réseaux de votre VPC. Les demandes adressées à Amazon S3 via les points de terminaison d'interface restent sur le réseau Amazon. Vous pouvez également accéder aux points de terminaison d'interface de votre VPC à partir d'applications sur site AWS Direct Connect via AWS Virtual Private Network ou ().AWS VPN Pour plus d'informations sur la façon de connecter votre VPC à votre réseau sur site, consultez le Guide de l'utilisateur AWS Direct Connect et le Guide de l'utilisateur AWS Site-to-Site VPN.

Pour des informations générales sur les points de terminaison d'interface, consultez Points de terminaison de VPC d'interface (AWS PrivateLink) dans le Guide AWS PrivateLink .

Rubriques

- Types de points de terminaison de VPC pour Amazon S3
- Restrictions et limites de AWS PrivateLink pour Amazon S3
- Création d'un point de terminaison d'un VPC
- Accès aux points de terminaison d'interface d'Amazon S3
- DNS privé
- Accès aux compartiments, aux points d'accès et aux opérations d'API de contrôle Amazon S3 depuis les points de terminaison de l'interface S3
- Mise à jour d'une configuration DNS sur site
- Création d'une stratégie de point de terminaison de VPC pour Amazon S3

Types de points de terminaison de VPC pour Amazon S3

Vous pouvez utiliser deux types de points de terminaison VPC pour accéder à Amazon S3 : les points de terminaison de passerelle et les points de terminaison d'interface (en utilisant). AWS PrivateLink Un point de terminaison de passerelle est une passerelle que vous spécifiez dans votre table de routage pour accéder à Amazon S3 depuis votre VPC via le AWS réseau. Les points de terminaison

d'interface étendent les fonctionnalités des points de terminaison de passerelle en utilisant des adresses IP privées pour acheminer les demandes vers Amazon S3 depuis votre VPC, sur site, ou depuis un VPC dans un autre en utilisant Région AWS le peering VPC ou. AWS Transit Gateway Pour plus d'informations, consultez Qu'est-ce que l'appairage de VPC ? et Transit Gateway vs VPC peering (Passerelle de transit ou appairage de VPC).

Les points de terminaison d'interface sont compatibles avec les points de terminaison de passerelle. Si vous avez un point de terminaison de passerelle existant dans votre VPC, vous pouvez utiliser les deux types de points de terminaison dans le même VPC.

Points de terminaison de passerelle pour Amazon S3	Points de terminaison d'interface pour Amazon S3
Dans les deux cas, votre trafic réseau reste sur le AWS réseau.	
Utiliser des adresses IP publiques Amazon S3	Utiliser des adresses IP privées depuis votre VPC pour accéder à Amazon S3
Utiliser les mêmes noms DNS Amazon S3	Exiger des noms DNS Amazon S3 spécifiques aux points de terminaison
N'autorise pas l'accès sur site	Autoriser l'accès depuis vos sites
Ne pas autoriser l'accès depuis un autre Région AWS	Autoriser l'accès d'un VPC à un autre en utilisant le Région AWS peering VPC ou AWS Transit Gateway
Non facturé	Facturé

Pour plus d'informations sur les points de terminaison de passerelle, consultez Points de terminaison de VPC de passerelle dans le Guide AWS PrivateLink .

Restrictions et limites de AWS PrivateLink pour Amazon S3

Les limites du VPC s'appliquent AWS PrivateLink à Amazon S3. Pour plus d'informations, consultez Considérations sur les points de terminaison d'interface et Quotas AWS PrivateLink dans le Guide AWS PrivateLink . En outre, les restrictions suivantes s'appliquent.

AWS PrivateLink pour Amazon S3 ne prend pas en charge les éléments suivants :

- Points de terminaison FIPS (Federal Information Processing Standard)
- Points de terminaison de sites web
- Points de terminaison globaux hérités
- Points de terminaison de la région S3 Dash
- Points de terminaison Dual-Stack
- En utilisant CopyObjectou UploadPartCopyentre des seaux dans différents Régions AWS
- Pprotocole TLS (Transport Layer Security) 1.0
- Protocole TLS (Transport Layer Security) 1.1
- Sécurité de la couche de transport (TLS) 1.3

Création d'un point de terminaison d'un VPC

Pour créer un point de terminaison d'interface de VPC, consultez Création d'un point de terminaison de VPC dans le Guide AWS PrivateLink .

Accès aux points de terminaison d'interface d'Amazon S3

Lorsque vous créez un point de terminaison d'interface, Amazon S3 génère deux types de noms DNS S3 spécifiques au point de terminaison : des noms Régionaux et des noms zonaux.

- Un nom DNS régional inclut un ID de point de terminaison VPC unique, un identifiant de service Région AWS, le et `vpce.amazonaws.com` dans son nom. Par exemple, pour l'ID de point de terminaison de VPC *`vpce-1a2b3c4d`*, le nom DNS généré peut être similaire à *`vpce-1a2b3c4d-5e6f`*`.s3.us-east-1.vpce.amazonaws.com`.
- Les noms DNS zonaux incluent la zone de disponibilité, par exemple, *`vpce-1a2b3c4d-5e6f`*`-`**`us-east-1a`**`.s3.us-east-1.vpce.amazonaws.com`. Vous pouvez utiliser cette option si votre architecture isole les zones de disponibilité. Par exemple, vous pouvez l'utiliser pour contenir les pannes ou réduire les coûts de transfert de données Régionaux.

Les noms DNS S3 spécifiques au point de terminaison peuvent être résolus depuis le domaine DNS public S3.

DNS privé

Les options de DNS privé pour les points de terminaison de l'interface d'un VPC simplifient le routage du trafic S3 vers les points de terminaison d'un VPC et vous aident à tirer parti du chemin

réseau le plus économique disponible pour votre application. Vous pouvez utiliser des options de DNS privé pour acheminer le trafic S3 régional sans mettre à jour vos clients S3 pour utiliser les noms DNS spécifiques aux points de terminaison de vos points de terminaison d'interface, ni gérer l'infrastructure DNS. Lorsque les noms DNS privés sont activés, les requêtes DNS S3 régionales sont résolues vers les adresses IP privées AWS PrivateLink des points de terminaison suivants :

- Points de terminaison régionaux de compartiment (par exemple, `s3.us-east-1.amazonaws.com`)
- Points de contrôle (par exemple, `s3-control.us-east-1.amazonaws.com`)
- Points de terminaison des points d'accès (par exemple, `s3-accesspoint.us-east-1.amazonaws.com`)

AWS PrivateLink pour Amazon S3 ne prend pas en charge l'utilisation de points de terminaison à double pile Amazon S3. Si vous utilisez un nom DNS S3 à double pile comme nom DNS privé, votre IPv6 trafic sera soit supprimé, soit, si votre cloud privé virtuel (VPC) possède une passerelle Internet, IPv6 votre trafic sera acheminé via la passerelle Internet de votre VPC.

Si votre VPC comporte un point de terminaison de passerelle, vous pouvez automatiquement acheminer les demandes internes au VPC via votre point de terminaison de passerelle S3 existant et les demandes sur site via le point de terminaison de votre interface. Cette approche vous permet d'optimiser vos coûts de mise en réseau en utilisant des points de terminaison de passerelle, qui ne sont pas facturés, pour votre trafic interne au VPC. Vos applications sur site peuvent être utilisées à l' AWS PrivateLink aide du point de terminaison Resolver entrant. Amazon fournit un serveur DNS pour votre VPC, appelé Route 53 Resolver. Un point de terminaison Resolver entrant réachemine des requêtes DNS à partir du réseau sur site vers Route 53 Resolver.

> **Important**
>
> Pour bénéficier du chemin réseau le plus économique lorsque vous utilisez l'option Activer le DNS privé uniquement pour les points de terminaison entrants, un point de terminaison de passerelle doit être présent dans votre VPC. La présence d'un point de terminaison de passerelle permet de garantir que le trafic interne au VPC passe toujours par le réseau privé d' AWS lorsque l'option Activer le DNS privé uniquement pour les points de terminaison entrants est sélectionnée. Vous devez conserver ce point de terminaison de passerelle tant que l'option Activer le DNS privé uniquement pour les points de terminaison entrants est sélectionnée. Si vous souhaitez supprimer le point de terminaison de votre passerelle, vous

devez d'abord désactiver Activer le DNS privé uniquement pour les points de terminaison entrants.
Si vous souhaitez mettre à jour un point de terminaison d'interface existant pour Activer le DNS privé uniquement pour les points de terminaison entrants, vérifiez d'abord que votre VPC possède un point de terminaison de passerelle S3. Pour plus d'informations sur les points de terminaison de passerelle et la gestion des noms DNS privés, consultez Points de terminaison de passerelle et Gestion des noms DNS privés dans le Guide AWS PrivateLink .

L'option Activer le DNS privé uniquement pour les points de terminaison entrants n'est disponible que pour les services qui prennent en charge les points de terminaison de passerelle.

Pour plus d'informations sur la création d'un point de terminaison d'un VPC utilisant l'option Activer le DNS privé uniquement pour les points de terminaison entrants, consultez Créer un point de terminaison d'interface dans le Guide AWS PrivateLink .

Utilisation de la console du VPC

Dans la console, vous avez deux options : Activer le nom DNS et Activer le DNS privé uniquement pour les points de terminaison entrants. Activer le nom DNS est une option prise en charge par AWS PrivateLink. En utilisant l'option Activer le nom DNS, vous pouvez utiliser la connectivité privée d'Amazon à Amazon S3, tout en envoyant des demandes aux noms DNS des points de terminaison publics par défaut. Lorsque cette option est activée, les clients peuvent bénéficier du chemin réseau le plus économique disponible pour leur application.

Lorsque vous activez les noms DNS privés sur un point de terminaison d'interface de VPC existant ou nouveau pour Amazon S3, l'option Activer le DNS privé uniquement pour les points de terminaison entrants est sélectionnée par défaut. Si cette option est sélectionnée, vos applications utilisent uniquement des points de terminaison d'interface pour votre trafic sur site. Ce trafic interne au VPC utilise automatiquement les points de terminaison de passerelle les moins coûteux. Vous pouvez également désactiver l'option Activer le DNS privé uniquement pour les points de terminaison entrants afin d'acheminer toutes les demandes S3 via le point de terminaison de votre interface.

À l'aide du AWS CLI

Si vous ne spécifiez pas de valeur pour `PrivateDnsOnlyForInboundResolverEndpoint`, la valeur par défaut est `true`. Toutefois, avant que votre VPC n'applique vos paramètres, il vérifie qu'un point de terminaison de passerelle est présent dans le VPC. Si un point de terminaison de passerelle est présent dans le VPC, l'appel aboutit. Sinon, le message d'erreur suivant s'affiche :

Pour que ce paramètre PrivateDnsOnlyForInboundResolverEndpoint soit défini sur true, le VPC *vpce_id* doit disposer d'un point de terminaison de passerelle pour le service.

Pour un nouveau point de terminaison d'interface de VPC

Utilisez les attributs `private-dns-enabled` et `dns-options` pour activer le DNS privé via la ligne de commande. L'option `PrivateDnsOnlyForInboundResolverEndpoint` de l'attribut `dns-options` doit être définie sur `true`. Remplacez *user input placeholders* par vos propres informations.

```
aws ec2 create-vpc-endpoint \
--region us-east-1 \
--service-name s3-service-name \
--vpc-id client-vpc-id \
--subnet-ids client-subnet-id \
--vpc-endpoint-type Interface  \
--private-dns-enabled  \
--ip-address-type ip-address-type \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true \
--security-group-ids client-sg-id
```

Pour un point de terminaison d'un VPC existant

Si vous souhaitez utiliser un DNS privé pour un point de terminaison d'un VPC existant, utilisez l'exemple de commande suivant et remplacez *user input placeholders* par vos propres informations.

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=false
```

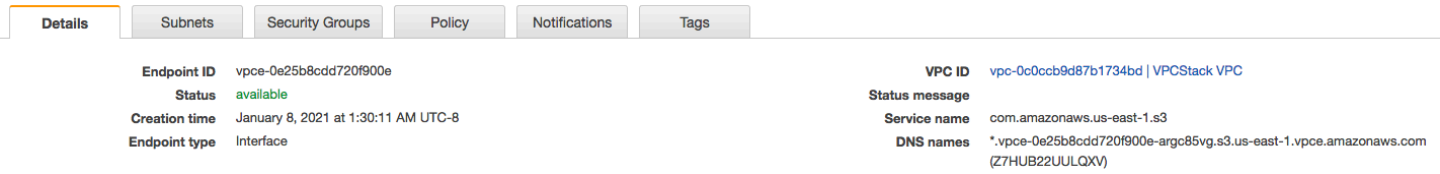
Si vous souhaitez mettre à jour un point de terminaison d'un VPC existant afin d'activer le DNS privé uniquement pour le résolveur entrant, utilisez l'exemple suivant et remplacez les exemples de valeurs par les vôtres.

```
aws ec2 modify-vpc-endpoint \
--region us-east-1 \
--vpc-endpoint-id client-vpc-id \
--private-dns-enabled \
--dns-options PrivateDnsOnlyForInboundResolverEndpoint=true
```

Accès aux compartiments, aux points d'accès et aux opérations d'API de contrôle Amazon S3 depuis les points de terminaison de l'interface S3

Vous pouvez utiliser le AWS CLI ou AWS SDKs pour accéder aux buckets, aux points d'accès S3 et aux opérations de l'API Amazon S3 Control via les points de terminaison de l'interface S3.

L'image suivante illustre l'onglet Détails de la console VPC, où vous pouvez trouver le nom DNS d'un point de terminaison de VPC. Dans cet exemple, l'ID de point de terminaison de VPC (vpce-id) est `vpce-0e25b8cdd720f900e` et le nom DNS est `*.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`.



Lorsque vous utilisez le nom DNS pour accéder à une ressource, remplacez-le `*` par la valeur appropriée. Les valeurs appropriées à utiliser à la place de `*` sont les suivantes :

- `bucket`
- `accesspoint`
- `control`

Par exemple, pour accéder à un compartiment, utilisez un nom DNS comme celui-ci :

`bucket.vpce-0e25b8cdd720f900e-argc85vg.s3.us-east-1.vpce.amazonaws.com`

Pour obtenir des exemples d'utilisation des noms DNS pour accéder aux compartiments, aux points d'accès et aux opérations d'API de contrôle Amazon S3, consultez les sections suivantes de AWS CLI exemples et AWS Exemples de SDK.

Pour plus d'informations sur la façon d'afficher vos noms DNS spécifiques aux terminaux, consultez Viewing endpoint service private DNS name configuration (Affichage de la configuration du nom DNS privé du service de point de terminaison) dans le Guide de l'utilisateur VPC.

AWS CLI exemples

Pour accéder aux compartiments S3, aux points d'accès S3 ou aux opérations de l'API Amazon S3 Control via les points de terminaison de l'interface S3 dans AWS CLI les commandes, utilisez les paramètres `--region` et`--endpoint-url`.

Exemple : utilisez une URL de point de terminaison pour répertorier les objets dans votre compartiment

Dans l'exemple suivant, remplacez le nom du compartiment *my-bucket*, la région *us-east-1* et le nom DNS de l'ID du point de terminaison de VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

```
aws s3 ls s3://my-bucket/ --region us-east-1 --endpoint-url
 https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
```

Exemple : utilisez une URL de point de terminaison pour répertorier les objets depuis un point d'accès

- Méthode 1 : utilisation de l'Amazon Resource Name (ARN) du point d'accès avec le point de terminaison du point d'accès

  Remplacez l'ARN *us-east-1:123456789012:accesspoint/accesspointexamplename*, la région *us-east-1* et l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

  ```
  aws s3api list-objects-v2 --bucket arn:aws:s3:us-east-1:123456789012:accesspoint/
  accesspointexamplename --region us-east-1 --endpoint-url
   https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com
  ```

  Si vous ne parvenez pas à exécuter correctement la commande, AWS CLI installez la dernière version et réessayez. Pour plus d'informations sur les instructions de mise à jour, consultez Installation ou mise à jour de la dernière version de l'interface AWS CLI dans le Guide de l'utilisateur AWS Command Line Interface .
- Méthode 2 : utilisation de l'alias du point d'accès avec le point de terminaison régional du compartiment

Dans l'exemple suivant, remplacez l'alias du point d'accès *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*, la région *us-east-1* et l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

```
aws s3api list-objects-v2 --
bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias
 --region us-east-1 --endpoint-url https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com
```

- Méthode 3 : utilisation de l'alias du point d'accès avec le point de terminaison du point d'accès

  Tout d'abord, pour construire un point de terminaison S3 avec le compartiment inclus dans le nom d'hôte, définissez le style d'adressage sur `virtual` pour `aws s3api`. Pour plus d'informations sur `AWS configure`, consultez Configuration and credential file settings (Paramètres des fichiers de configuration et d'informations d'identification) dans le Guide de l'utilisateur AWS Command Line Interface .

  ```
  aws configure set default.s3.addressing_style virtual
  ```

  Ensuite, dans l'exemple suivant, remplacez l'alias du point d'accès *accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias*, la région *us-east-1* et l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations. Pour plus d'informations sur les alias de point d'accès, consultez Alias de point d'accès.

  ```
  aws s3api list-objects-v2 --
  bucket accesspointexamplename-8tyekmigicmhun8n9kwpfur39dnw4use1a-s3alias --
  region us-east-1 --endpoint-url https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
  east-1.vpce.amazonaws.com
  ```

Exemple : utilisez une URL de point de terminaison pour répertorier les tâches avec une opération d'API de contrôle S3

Dans l'exemple suivant, remplacez la région *us-east-1*, l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* et l'ID du compte *12345678* par vos propres informations.

```
aws s3control --region us-east-1 --endpoint-url
 https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com list-jobs --
account-id 12345678
```

AWS Exemples de SDK

Pour accéder aux compartiments S3, aux points d'accès S3 ou aux opérations de l'API Amazon S3 Control via les points de terminaison de l'interface S3 lorsque vous utilisez le AWS SDKs, installez SDKs la dernière version. Configurez ensuite vos clients pour qu'ils utilisent une URL de point de terminaison afin d'accéder à un compartiment, un point d'accès ou des opérations d'API de contrôle Amazon S3 via des points de terminaison d'interface S3.

SDK for Python (Boto3)

Exemple : Utiliser une URL de point de terminaison pour accéder à un compartiment S3

Dans l'exemple suivant, remplacez la région *us-east-1* et l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

```
s3_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

Exemple : Utiliser une URL de point de terminaison pour accéder à un point d'accès S3

Dans l'exemple suivant, remplacez la région *us-east-1* et l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

```
ap_client = session.client(
service_name='s3',
region_name='us-east-1',
endpoint_url='https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com'
)
```

Exemple : utilisez une URL de point de terminaison pour accéder à l'API de contrôle Amazon S3

Dans l'exemple suivant, remplacez la région *us-east-1* et l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

```
control_client = session.client(
service_name='s3control',
region_name='us-east-1',
endpoint_url='https://control.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com'
)
```

SDK for Java 1.x

Exemple : Utiliser une URL de point de terminaison pour accéder à un compartiment S3

Dans l'exemple suivant, remplacez l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

```
// bucket client
final AmazonS3 s3 = AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://bucket.vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
List<Bucket> buckets = s3.listBuckets();
```

Exemple : Utiliser une URL de point de terminaison pour accéder à un point d'accès S3

Dans l'exemple suivant, remplacez l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* et l'ARN *us-east-1:123456789012:accesspoint/prod* par vos propres informations.

```
// accesspoint client
final AmazonS3 s3accesspoint =
 AmazonS3ClientBuilder.standard().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
ObjectListing objects = s3accesspoint.listObjects("arn:aws:s3:us-
east-1:123456789012:accesspoint/prod");
```

Exemple : utilisez une URL de point de terminaison pour accéder à une opération d'API de contrôle Amazon S3

Dans l'exemple suivant, remplacez l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* par vos propres informations.

```
// control client
final AWSS3Control s3control =
 AWSS3ControlClient.builder().withEndpointConfiguration(
        new AwsClientBuilder.EndpointConfiguration(
                "https://control.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com",
                Regions.DEFAULT_REGION.getName()
        )
).build();
final ListJobsResult jobs = s3control.listJobs(new ListJobsRequest());
```

SDK for Java 2.x

Exemple : Utiliser une URL de point de terminaison pour accéder à un compartiment S3

Dans l'exemple suivant, remplacez l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* et la région *Region.US_EAST_1* par vos propres informations.

```
// bucket client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://bucket.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com"))
                   .build()
```

Exemple : Utiliser une URL de point de terminaison pour accéder à un point d'accès S3

Dans l'exemple suivant, remplacez l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* et la région *Region.US_EAST_1* par vos propres informations.

```
// accesspoint client
Region region = Region.US_EAST_1;
s3Client = S3Client.builder().region(region)

 .endpointOverride(URI.create("https://accesspoint.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com"))
```

```
                    .build()
```

Exemple : utilisez une URL de point de terminaison pour accéder à l'API de contrôle Amazon S3

Dans l'exemple suivant, remplacez l'ID du point de terminaison d'un VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* et la région *Region.US_EAST_1* par vos propres informations.

```
// control client
Region region = Region.US_EAST_1;
s3ControlClient = S3ControlClient.builder().region(region)

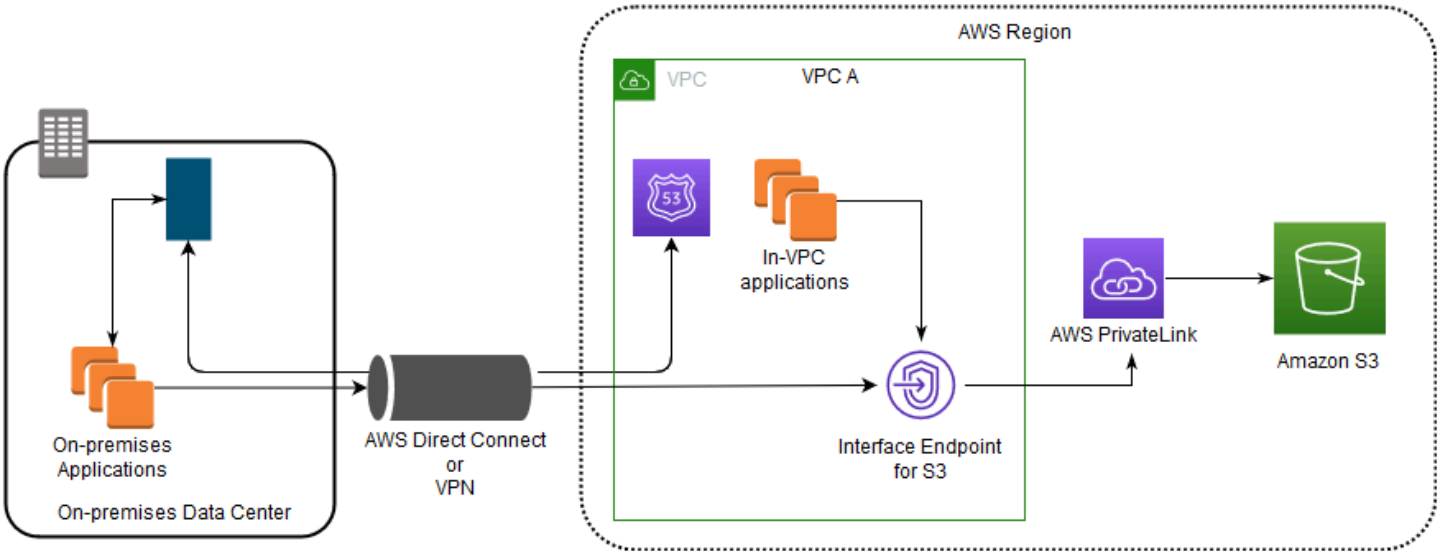
 .endpointOverride(URI.create("https://control.vpce-1a2b3c4d-5e6f.s3.us-
east-1.vpce.amazonaws.com"))
                                  .build()
```

Mise à jour d'une configuration DNS sur site

Lorsque vous utilisez des noms DNS spécifiques aux points de terminaison pour accéder aux points de terminaison d'interface pour Amazon S3, vous n'avez pas besoin de mettre à jour votre résolveur DNS sur site. Vous pouvez résoudre le nom DNS spécifique au point de terminaison avec l'adresse IP privée du point de terminaison d'interface depuis le domaine DNS public Amazon S3.

Utilisation de points de terminaison d'interface pour accéder à Amazon S3 sans point de terminaison de passerelle ou passerelle Internet dans le VPC

Les points de terminaison d'interface de votre VPC peuvent acheminer les applications de VPC et les applications sur site vers Amazon S3 via le réseau Amazon, comme illustré dans le diagramme suivant.

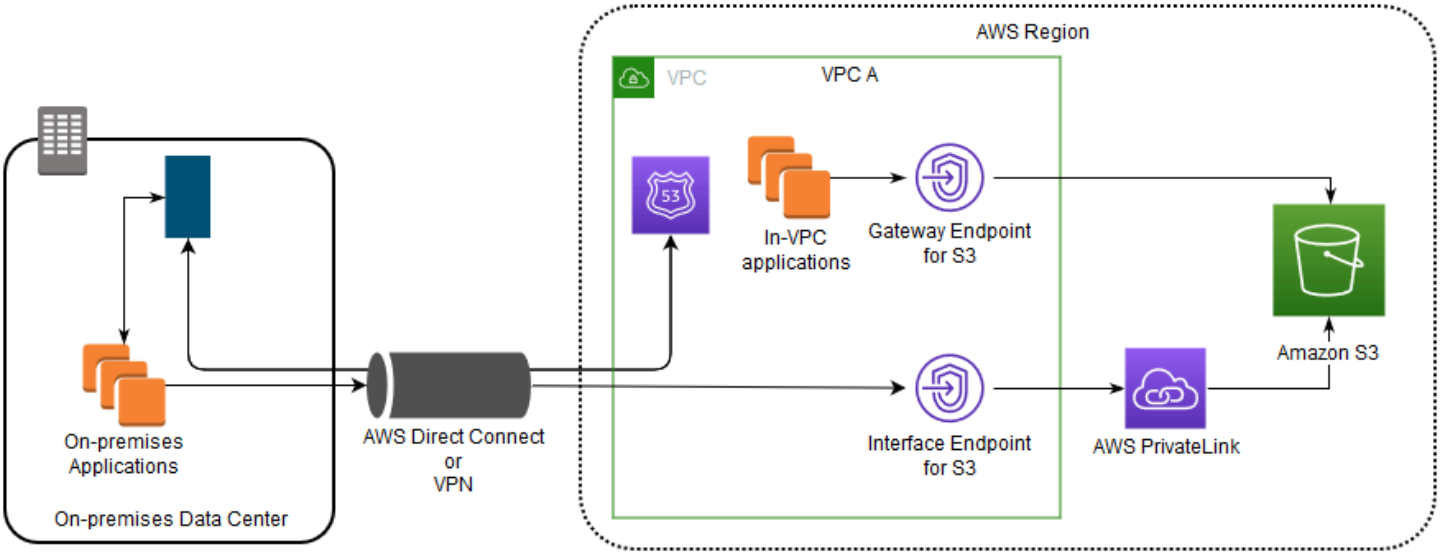


Le diagramme illustre les éléments suivants :

- Votre réseau local utilise AWS Direct Connect ou AWS VPN pour se connecter au VPC A.
- Vos applications sur site et dans le VPC A utilisent des noms DNS spécifiques aux points de terminaison pour accéder à Amazon S3 via le point de terminaison d'interface S3.
- Les applications locales envoient des données au point de terminaison de l'interface dans le VPC AWS Direct Connect via (ou) AWS VPN. AWS PrivateLink déplace les données du point de terminaison de l'interface vers Amazon S3 via le AWS réseau.
- Les applications in-VPC envoient également du trafic vers le point de terminaison de l'interface. AWS PrivateLink déplace les données du point de terminaison de l'interface vers Amazon S3 via le AWS réseau.

Utilisation conjointe de points de terminaison de passerelle et de points de terminaison d'interface dans le même VPC pour accéder à Amazon S3

Vous pouvez créer des points de terminaison d'interface et conserver le point de terminaison de passerelle existant dans le même VPC, comme le montre le diagramme suivant. En adoptant cette approche, vous autorisez les applications internes au VPC à continuer d'accéder à Amazon S3 via le point de terminaison de la passerelle, ce qui n'est pas facturé. Ensuite, seules vos applications sur site utilisent des points de terminaison d'interface pour accéder à Amazon S3. Pour accéder à Amazon S3 de cette façon, vous devez mettre à jour vos applications sur site afin d'utiliser des noms DNS spécifiques du point de terminaison pour Amazon S3.



Le diagramme illustre les éléments suivants :

- Les applications locales utilisent des noms DNS spécifiques au point de terminaison pour envoyer des données au point de terminaison de l'interface au sein du VPC via (ou). AWS Direct Connect AWS VPN AWS PrivateLink déplace les données du point de terminaison de l'interface vers Amazon S3 via le AWS réseau.
- À l'aide des noms régionaux Amazon S3 par défaut, les applications intégrées au VPC envoient des données au point de terminaison de la passerelle qui se connecte à Amazon S3 via le AWS réseau.

Pour plus d'informations sur les points de terminaison de passerelle, consultez Points de terminaison d'un VPC de passerelle dans le Guide de l'utilisateur VPC.

Création d'une stratégie de point de terminaison de VPC pour Amazon S3

Vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison de VPC qui contrôle l'accès à Amazon S3. La stratégie spécifie les informations suivantes :

- Le principal AWS Identity and Access Management (IAM) qui peut effectuer des actions
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles les actions peuvent être exécutées.

Vous pouvez également utiliser des stratégies de compartiment Amazon S3 pour restreindre l'accès à des compartiments spécifiques depuis un point de terminaison d'un VPC spécifique en utilisant la

condition `aws:sourceVpce` de votre politique de compartiment. Les exemples suivants montrent les stratégies qui restreignent l'accès à un compartiment ou à un point de terminaison.

Rubriques

- Exemple : restriction de l'accès à un compartiment spécifique depuis le point de terminaison d'un VPC
- Exemple : restriction de l'accès aux compartiments dans un compte spécifique depuis le point de terminaison d'un VPC
- Exemple : restriction de l'accès au point de terminaison d'un VPC spécifique dans la politique de compartiment S3

Exemple : restriction de l'accès à un compartiment spécifique depuis le point de terminaison d'un VPC

Vous pouvez créer une stratégie de point de terminaison qui restreint l'accès à des compartiments Amazon S3 spécifiques uniquement. Ce type de politique est utile si d'autres Services AWS politiques de votre VPC utilisent des buckets. La politique de compartiment suivante restreint l'accès à *amzn-s3-demo-bucket1* uniquement. Pour utiliser cette politique de point de terminaison, remplacez *amzn-s3-demo-bucket1* par le nom de votre compartiment.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909151",
  "Statement": [
    { "Sid": "Access-to-specific-bucket-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Allow",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket1",
                   "arn:aws:s3:::amzn-s3-demo-bucket1/*"]
    }
  ]
}
```

Exemple : restriction de l'accès aux compartiments dans un compte spécifique depuis le point de terminaison d'un VPC

Vous pouvez créer une politique de point de terminaison qui restreint l'accès uniquement aux compartiments S3 d'un point spécifique. Compte AWS Pour empêcher les clients de votre VPC d'accéder aux compartiments dont vous n'êtes pas le propriétaire, utilisez la déclaration suivante dans votre stratégie de point de terminaison. L'exemple de déclaration suivant crée une stratégie qui restreint l'accès aux ressources appartenant à un seul ID de Compte AWS , *111122223333*.

```
{
  "Statement": [
    {
      "Sid": "Access-to-bucket-in-specific-account-only",
      "Principal": "*",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Effect": "Deny",
      "Resource": "arn:aws:s3:::*",
      "Condition": {
        "StringNotEquals": {
          "aws:ResourceAccount": "111122223333"
        }
      }
    }
  ]
}
```

> **Note**
>
> Pour spécifier l' Compte AWS ID de la ressource à laquelle vous accédez, vous pouvez utiliser la clé `aws:ResourceAccount` ou la `s3:ResourceAccount` clé dans votre politique IAM. Sachez toutefois que certains Services AWS dépendent de l'accès à des buckets AWS gérés. Par conséquent, l'utilisation de la clé `aws:ResourceAccount` ou `s3:ResourceAccount` dans votre politique IAM risque également d'avoir un impact sur l'accès à ces ressources.

Exemple : restriction de l'accès au point de terminaison d'un VPC spécifique dans la politique de compartiment S3

Exemple : restriction de l'accès au point de terminaison d'un VPC spécifique dans la politique de compartiment S3

La politique de compartiment Amazon S3 suivante autorise l'accès à un compartiment spécifique, *amzn-s3-demo-bucket2*, depuis le point de terminaison d'un VPC *vpce-1a2b3c4d* uniquement. La politique refuse tout accès au compartiment si le point de terminaison spécifié n'est pas utilisé. La condition `aws:sourceVpce` spécifie le point de terminaison et ne requiert pas d'Amazon Resource Name (ARN) pour la ressource de point de terminaison d'un VPC, mais uniquement l'ID du point de terminaison. Pour utiliser cette stratégie de point de terminaison, remplacez *amzn-s3-demo-bucket2* et *vpce-1a2b3c4d* par le nom et le point de terminaison de votre compartiment.

> **Important**
>
> - Lors de l'application de la politique de compartiment Amazon S3 suivante afin de restreindre l'accès à certains points de terminaison d'un VPC uniquement, vous pouvez bloquer involontairement votre accès au compartiment. Les stratégies de compartiment dans le but de restreindre l'accès aux connexions issues du point de terminaison de votre VPC peuvent bloquer toutes les connexions à ce compartiment. Pour des informations sur la correction de ce problème, consultez Ma politique de compartiment n'a pas le bon VPC ou ID de point de terminaison d'un VPC. Comment puis-je corriger la politique de façon à pouvoir accéder au compartiment ? que vous trouverez dans le Support Centre de connaissances.
> - Avant d'utiliser l'exemple de stratégie suivant, remplacez l'ID de point de terminaison du VPC par une valeur appropriée pour votre cas d'utilisation. Dans le cas contraire, vous ne parviendrez pas à accéder à votre compartiment.
> - Cette politique désactive l'accès de la console au compartiment spécifié, car les demandes de la console ne proviennent pas du point de terminaison du VPC défini.

JSON

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

```
  "Id": "Policy1415115909152",
  "Statement": [
    { "Sid": "Access-to-specific-VPCE-only",
      "Principal": "*",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": ["arn:aws:s3:::amzn-s3-demo-bucket2",
                   "arn:aws:s3:::amzn-s3-demo-bucket2/*"],
      "Condition": {"StringNotEquals": {"aws:sourceVpce": "vpce-1a2b3c4d"}}
    }
  ]
}
```

Pour plus d'exemples de stratégie, consultez Points de terminaison pour Amazon S3 dans le Guide de l'utilisateur VPC.

Pour plus d'informations sur la connectivité VPC, consultez les options de Network-to-VPC connectivité dans le AWS livre blanc Amazon Virtual Private Cloud Connectivity Options.

Validation de conformité pour Amazon S3

La sécurité et la conformité d'Amazon S3 sont évaluées par des auditeurs tiers dans le cadre de plusieurs programmes de AWS conformité, notamment les suivants :

- System and Organization Controls (SOC)
- Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)
- Federal Risk and Authorization Management Program (FedRAMP)
- Health Insurance Portability and Accountability Act (HIPAA)

AWS fournit une liste fréquemment mise à jour des AWS services concernés par des programmes de conformité spécifiques sur la page AWS Services in Scope by Compliance Program.

Les rapports d'audit tiers peuvent être téléchargés à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact.

Pour plus d'informations sur les programmes de AWS conformité, consultez AWS la section Programmes de conformité.

Votre responsabilité de conformité lors de l'utilisation d'Amazon S3 est déterminée par la sensibilité de vos données, les objectifs de conformité de votre organisation, ainsi que par la législation et la réglementation applicables. Si votre utilisation d'Amazon S3 est soumise à la conformité à des normes telles que HIPAA, PCI, ou FedRAMP, AWS fournit des ressources pour vous aider :

- Guides de démarrage rapide sur la sécurité et la conformité qui abordent les considérations architecturales et les étapes à suivre pour déployer des environnements de base axés sur la sécurité et la conformité sur. AWS
- Architecting for HIPAA Security and Compliance décrit la manière dont les entreprises les aident AWS à répondre aux exigences de la HIPAA.
- AWS Les ressources de conformité fournissent plusieurs classeurs et guides différents qui peuvent s'appliquer à votre secteur d'activité et à votre région.
- Le service AWS Config peut permettre d'évaluer comment les configurations de vos ressources se conforment aux pratiques internes, aux normes et aux directives industrielles.
- AWS Security Hub vous fournit une vue complète de l'état de votre sécurité interne AWS et vous aide à vérifier votre conformité aux normes et aux meilleures pratiques du secteur de la sécurité.
- Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet peut vous aider à répondre aux exigences techniques de régulateurs des services financiers (comme les organismes SEC, FINRA

et CFTC) qui exigent un stockage des données en écriture seule et lectures multiples (WORM) pour certains types de document et informations d'enregistrement.

- Catalogage et analyse de vos données avec l'inventaire S3 peut vous aider à auditer et signaler le statut de réplication et de chiffrement de vos objets à des fins professionnelles, de conformité et d'obligations réglementaires.

Résilience dans Amazon S3

L'infrastructure AWS mondiale est construite autour des régions et des zones de disponibilité. Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées connectées par un réseau à faible latence, à haut débit et hautement redondant. Ces zones de disponibilité vous offrent un moyen efficace de concevoir et d'exploiter des applications et des bases de données. Elles sont plus hautement disponibles, tolérantes aux pannes et évolutives que les infrastructures traditionnelles à un ou plusieurs centres de données. Si vous avez spécifiquement besoin de répliquer vos données sur de plus grandes distances géographiques, vous pouvez utiliser Réplication d'objets au sein des régions et entre elles ce qui permet de copier automatiquement et de manière asynchrone des objets entre des compartiments situés dans différents compartiments. Régions AWS

Chacune Région AWS possède plusieurs zones de disponibilité. Vous pouvez déployer vos applications dans plusieurs zones de disponibilité au sein d'une même Région pour bénéficier d'une tolérance aux pannes et d'une faible latence. Les zones de disponibilité sont connectées les unes aux autres via une mise en réseau à fibres optiques rapide et privée, ce qui nous permet de concevoir facilement des applications qui basculent automatiquement entre les zones de disponibilité sans interruption.

Pour plus d'informations sur les zones de disponibilité Régions AWS et les zones de disponibilité, consultez la section Infrastructure AWS globale.

Outre l'infrastructure AWS mondiale, Amazon S3 propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données.

Configuration du cycle de vie

> Une configuration du cycle de vie est un ensemble de règles qui définit des action qu'Amazon S3 applique à un groupe d'objets. Avec des règles de configuration du cycle de vie, vous pouvez indiquer à Amazon S3 de passer à des classes de stockage moins onéreuses, de les archiver ou de les supprimer. Pour plus d'informations, consultez Gestion du cycle de vie des objets.

Gestion des versions

> La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. Le contrôle de version permet de récupérer facilement les données en cas d'actions involontaires des utilisateurs

ou de défaillances des applications. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Verrouillage des objets S3

La fonctionnalité de verrouillage des objets S3 vous permet de stocker des objets selon un modèle WORM write once, read many. En utilisant le verrouillage des objets S3, vous pouvez empêcher qu'un objet soit supprimé ou remplacé sur une période déterminée ou indéfinie. La fonctionnalité de verrouillage des objets S3 vous permet de satisfaire aux exigences réglementaires qui nécessitent le stockage WORM, ou de simplement ajouter une couche supplémentaire de protection contre la suppression et les modifications d'objet. Pour plus d'informations, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

Classes de stockage

Amazon S3 offre une gamme de classes de stockage à choisir en fonction des exigences de votre charge de travail. Les classes de stockage S3 Standard-IA et S3 One Zone-IA sont conçues pour les données auxquelles vous accédez environ une fois par mois et nécessitent un accès en millisecondes. La classe de stockage S3 Glacier Instant Retrieval est conçue pour les données d'archivage de longue durée accessibles avec un accès en millisecondes auxquelles vous accédez environ une fois par trimestre. Pour les données d'archivage qui ne nécessitent pas d'accès immédiat, telles que les sauvegardes, vous pouvez utiliser les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour plus d'informations, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

Les bonnes pratiques de sécurité suivantes s'appliquent également à la résilience :

- Enable versioning
- Consider Amazon S3 cross-region replication
- Identify and audit all your Amazon S3 buckets

Chiffrement des sauvegardes Amazon S3

Si vous stockez des sauvegardes à l'aide d'Amazon S3, le chiffrement de vos sauvegardes dépend de la configuration de ces compartiments. Amazon S3 fournit un moyen de définir le comportement de chiffrement par défaut pour un compartiment S3. Vous pouvez définir le chiffrement par défaut sur un compartiment afin que tous les objets soient chiffrés lorsqu'ils sont stockés dans le compartiment. Le chiffrement par défaut prend en charge les clés stockées dans AWS KMS (SSE-KMS). Pour de plus amples informations, veuillez consulter Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.

Pour en savoir plus sur la gestion des versions et le verrouillage des objets, consultez les rubriques suivantes : Conservation de plusieurs versions d'objets grâce à la gestion des versions S3 Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet

Sécurité de l'infrastructure dans Amazon S3

En tant que service géré, Amazon S3 est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le pilier de sécurité du AWS Well-Architected Framework.

L'accès à Amazon S3 via le réseau se fait via la AWS publication APIs. Les clients doivent prendre en charge le protocole TLS (Transport Layer Security) 1.2. Nous recommandons également la prise en charge de TLS 1.3. (Pour plus d'informations sur cette recommandation, consultez la section Connexions AWS cloud plus rapides avec TLS 1.3 sur le blog AWS de sécurité.)

> **Note**
>
> Le protocole TLS 1.3 est pris en charge sur tous les points de terminaison S3, à l' AWS PrivateLink exception d'Amazon S3 et des points d'accès multirégionaux.

Les clients doivent également prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE) ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). En outre, les demandes doivent être signées à l'aide de AWS la signature V4 ou de AWS la signature V2, ce qui nécessite la fourniture d'informations d'identification valides.

Ils APIs sont appelables depuis n'importe quel emplacement du réseau. Toutefois, Amazon S3 prend bel et bien en charge les stratégies d'accès basées sur les ressources, ce qui peut inclure des restrictions en fonction de l'adresse IP source. Vous pouvez également utiliser les politiques relatives aux compartiments Amazon S3 pour contrôler l'accès aux compartiments à partir de points de terminaison de cloud privé virtuel (VPC) spécifiques, ou spécifiques. VPCs En fait, cela isole l'accès réseau à un compartiment Amazon S3 donné uniquement du VPC spécifique au sein AWS du réseau. Pour de plus amples informations, veuillez consulter Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment.

Les bonnes pratiques de sécurité suivantes s'appliquent également à la sécurité de l'infrastructure dans Amazon S3 :

- Consider VPC endpoints for Amazon S3 access
- Identify and audit all your Amazon S3 buckets

Configuration et analyse des vulnérabilités dans Amazon S3

AWS gère les tâches de sécurité de base telles que l'application de correctifs au système d'exploitation client (OS) et aux bases de données, la configuration du pare-feu et la reprise après sinistre. Ces procédures ont été vérifiées et certifiées par les tiers appropriés. Pour plus de détails, consultez les ressources suivantes :

- Validation de conformité pour Amazon S3
- Modèle de responsabilité partagée
- Amazon Web Services : Présentation des procédures de sécurité

Les bonnes pratiques de sécurité suivantes s'appliquent également à la configuration et à l'analyse des vulnérabilités dans Amazon S3 :

- Identify and audit all your Amazon S3 buckets
- Activer AWS Config

Gestion des accès

Amazon S3 fournit divers outils de gestion des accès. Vous trouverez ci-dessous une liste de ces fonctionnalités et outils. Vous n'avez pas besoin de tous ces outils de gestion des accès, mais vous devez en utiliser un ou plusieurs pour accorder l'accès à vos compartiments et objets Amazon S3, ainsi qu'aux autres Ressources S3. Une utilisation adéquate de ces outils contribue à garantir que vos ressources ne sont accessibles qu'aux utilisateurs prévus.

L'outil de gestion des accès le plus couramment utilisé est une stratégie d'accès. Une politique d'accès peut être une politique basée sur les ressources attachée à une AWS ressource, telle qu'une politique de compartiment pour un compartiment. Une stratégie d'accès peut également être une politique basée sur l'identité. Dans ce cas, elle est associée à une identité AWS Identity and Access Management (IAM), telle qu'un utilisateur, un groupe ou un rôle IAM. Une stratégie d'accès décrit qui a accès à quoi. Rédigez une politique d'accès pour accorder Comptes AWS aux utilisateurs, aux groupes et aux rôles IAM l'autorisation d'effectuer des opérations sur une ressource. Par exemple, vous pouvez accorder une `PUT Object` autorisation à un autre compte Compte AWS afin qu'il puisse télécharger des objets dans votre compartiment.

Les outils de gestion de l'accès disponibles dans Amazon S3 sont les suivants. Pour obtenir un guide plus complet sur le contrôle d'accès Amazon S3, consultez Contrôle d'accès dans Amazon S3.

Politique de compartiment

Une politique de compartiment Amazon S3 est une politique AWS Identity and Access Management (IAM) basée sur les ressources, au format JSON. Elle est associée à un compartiment particulier. Utilisez des politiques de compartiment pour accorder des autorisations à d'autres identités Comptes AWS ou à des identités IAM pour le compartiment et les objets qu'il contient. De nombreux cas d'utilisation de la gestion des accès S3 peuvent être satisfaits au moyen d'une politique de compartiment. Avec les politiques de compartiment, vous pouvez personnaliser l'accès au compartiment pour vous assurer que seules les identités que vous avez approuvées peuvent accéder aux ressources et effectuer des actions en leur sein. Pour de plus amples informations, veuillez consulter Politiques de compartiment pour Amazon S3.

Politique basée sur l'identité

Une politique utilisateur IAM ou basée sur l'identité est un type de politique AWS Identity and Access Management (IAM). Une politique basée sur l'identité est une politique au format JSON associée aux utilisateurs, groupes ou rôles IAM dans votre compte AWS . Vous pouvez utiliser des politiques basées sur l'identité pour accorder à une identité IAM l'accès à vos compartiments ou objets. Vous pouvez créer des utilisateurs, des groupes et des rôles IAM dans votre compte et leur attacher des stratégies d'accès. Vous pouvez ensuite accorder l'accès aux ressources AWS , notamment aux ressources Amazon S3. Pour de plus amples informations, veuillez consulter Politiques basées sur l'identité pour Amazon S3.

Autorisations d'accès S3

Utilisez les autorisations d'accès S3 pour créer des autorisations d'accès à vos données Amazon S3 pour les identités figurant dans les annuaires d'identités d'entreprise, telles qu'Active Directory, et les identités AWS Identity and Access Management (IAM). Les autorisations d'accès S3 vous aident à gérer les autorisations de données à l'échelle. En outre, les autorisations d'accès S3 enregistrent l'identité de l'utilisateur final et l'application utilisée pour accéder aux données S3 dans AWS CloudTrail. Cela fournit un historique d'audit détaillé remontant jusqu'à l'identité de l'utilisateur final pour tous les accès aux données de vos compartiments S3. Pour de plus amples informations, veuillez consulter Gestion de l'accès avec les autorisations d'accès S3.

Points d'accès

Les points d'accès Amazon S3 simplifient la gestion de l'accès aux données à l'échelle pour les applications utilisant des jeux de données partagés dans S3. Les points d'accès sont appelés points de terminaison réseau. Ils sont associés à un compartiment. Vous pouvez utiliser des points d'accès pour effectuer des opérations sur des objets S3 à l'échelle, comme le chargement et l'extraction

d'objets. Jusqu'à 10 000 points d'accès peuvent être associés à un compartiment. Et pour chaque point d'accès, vous pouvez appliquer des autorisations et des contrôles réseau distincts pour vous donner un contrôle précis sur l'accès à vos objets S3. Les points d'accès S3 peuvent être associés à des compartiments du même compte ou d'un autre compte approuvé. Les stratégies de points d'accès sont basées sur les ressources. Elles sont évaluées conjointement avec la politique de compartiment sous-jacente. Pour de plus amples informations, veuillez consulter Gestion de l'accès aux jeux de données avec des points d'accès .

Liste de contrôle d'accès (ACL)

Une ACL est une liste de subventions identifiant le bénéficiaire et l'autorisation accordée. ACLs accorder des autorisations de lecture ou d'écriture de base à d'autres Comptes AWS. ACLs utilisez un schéma XML spécifique à Amazon S3. Une liste ACL est un type de politique AWS Identity and Access Management (IAM). Une liste ACL d'objet est utilisée pour gérer l'accès à un objet, tandis qu'une liste ACL de compartiment est utilisée pour gérer l'accès à un compartiment. Avec les politiques de compartiment, il existe une seule politique pour l'ensemble du compartiment, mais ACLs les objets sont spécifiés pour chaque objet. Nous vous recommandons de rester ACLs éteint, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès individuellement pour chaque objet. Pour plus d'informations sur l'utilisation ACLs, consultezContrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

> **Warning**
>
> La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent pas l'utilisation de ACLs.

Propriétaire de l'objet

Pour gérer l'accès à vos objets, vous devez en être le propriétaire. Utilisez le paramètre Propriétaire de l'objet au niveau du compartiment pour contrôler la propriété des objets chargés dans votre compartiment. Utilisez également la propriété des objets pour l'activer ACLs. Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket et tous les paramètres ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère exclusivement l'accès aux données. Pour gérer l'accès, le propriétaire du compartiment utilise des politiques ou un autre outil de gestion des accès, à l'exception de ACLs. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Pour obtenir un guide plus complet sur le contrôle d'accès Amazon S3 et d'autres bonnes pratiques, consultez Contrôle d'accès dans Amazon S3.

Protection des données dans Amazon S3

Outre la résilience offerte par l'infrastructure AWS mondiale, Amazon S3 propose un certain nombre de fonctionnalités permettant de protéger vos données contre les suppressions accidentelles ou les défaillances régionales.

Réplication S3

La réplication en direct permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3. Les buckets configurés pour la réplication d'objets peuvent appartenir au même compte Compte AWS ou à des comptes différents. Vous pouvez répliquer des objets vers un compartiment de destination unique ou plusieurs compartiments de destination. Les compartiments de destination peuvent se trouver dans une région différente Régions AWS ou dans la même région que le compartiment source. Pour activer les contrôles de basculement, vous pouvez configurer la réplication pour qu'elle soit bidirectionnelle, afin que vos compartiments sources et de destination puissent rester synchronisés en cas de panne régionale. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets au sein des régions et entre elles".

Points d'accès multi-régions et contrôles de basculement

Les points d'accès multi-régions Amazon S3 fournissent un point de terminaison global que les applications peuvent utiliser pour traiter les demandes provenant de compartiments S3 situés dans plusieurs Régions AWS. Vous pouvez utiliser des points d'accès multi-régions pour créer des applications multi-régions avec la même architecture utilisée dans une seule région, puis exécuter ces applications partout dans le monde. Au lieu d'envoyer les demandes sur l'Internet public encombré, les points d'accès multi-régions offrent une résilience de réseau intégrée avec une accélération des demandes Internet vers Amazon S3. Les demandes d'application adressées à un point de terminaison global de point d'accès multi-régions utilisent AWS Global Accelerator pour acheminer automatiquement sur le réseau mondial AWS vers le compartiment S3 le plus proche ayant un statut d'acheminement actif. Pour plus d'informations sur les points d'accès multi-régions, consultez the section called "Gestion du trafic multirégional ".

Grâce aux contrôles de basculement du point d'accès multi-régions d'Amazon S3, vous pouvez maintenir la continuité des activités pendant les perturbations du trafic régional, tout en offrant à vos applications une architecture multi-régions pour répondre aux besoins de conformité et de redondance. Si votre trafic régional est perturbé, vous pouvez utiliser les contrôles de basculement des points d'accès multirégionaux pour sélectionner celui situé Régions AWS

derrière un point d'accès multirégional Amazon S3 qui traitera les demandes d'accès aux données et de stockage.

Pour prendre en charge le basculement, vous pouvez configurer votre point d'accès multi-régions dans une configuration active-passive, le trafic circulant vers la région active dans des conditions normales, et une région passive de secours pour le basculement. Si vous avez activé la réplication entre régions (CRR) de S3 avec des règles de réplication bidirectionnelle, vous pouvez garder vos compartiments synchronisés pendant un basculement. Pour plus d'informations sur les contrôles de basculement, consultez the section called "Configuration du basculement".

Gestion des versions S3

La gestion des versions est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Amazon S3. Le contrôle de version permet de récupérer facilement les données en cas d'actions involontaires des utilisateurs ou de défaillances des applications. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Verrouillage des objets S3

La fonctionnalité de verrouillage des objets S3 vous permet de stocker des objets selon un modèle WORM write once, read many. En utilisant le verrouillage des objets S3, vous pouvez empêcher qu'un objet soit supprimé ou remplacé sur une période déterminée ou indéfinie. La fonctionnalité de verrouillage des objets S3 vous permet de satisfaire aux exigences réglementaires qui nécessitent le stockage WORM, ou de simplement ajouter une couche supplémentaire de protection contre la suppression et les modifications d'objet. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

AWS Backup

Amazon S3 est intégré de manière native à AWS Backup un service entièrement géré basé sur des politiques que vous pouvez utiliser pour définir de manière centralisée des politiques de sauvegarde afin de protéger vos données dans Amazon S3. Après avoir défini vos politiques de sauvegarde et affecté les ressources Amazon S3 aux politiques, vous AWS Backup automatisez la création de sauvegardes Amazon S3 et les stockez de manière sécurisée dans un coffre-fort de sauvegarde crypté que vous désignez dans votre plan de sauvegarde. Pour de plus amples informations, veuillez consulter the section called "Sauvegarde des données".

Pour un tutoriel sur l'utilisation conjointe de certaines de ces fonctionnalités afin de protéger vos données, consultez Didacticiel : Protéger les données sur Amazon S3 des suppressions accidentelles ou des bogues de l'application avec la gestion des versions S3, le verrouillage d'objet S3 et la réplication S3.

> **Important**
>
> Outre l'utilisation des fonctionnalités précédentes pour protéger vos données, nous vous recommandons de consulter les recommandations fournies dans the section called "Bonnes pratiques de sécurité".

Rubriques

- Réplication d'objets au sein des régions et entre elles
- Gestion du trafic multirégional avec des points d'accès multirégionaux
- Conservation de plusieurs versions d'objets grâce à la gestion des versions S3
- Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet
- Sauvegarde de vos données Amazon S3

Réplication d'objets au sein des régions et entre elles

La réplication permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3. Les compartiments configurés pour la réplication d'objet peuvent appartenir au même Compte AWS ou à des comptes distincts. Vous pouvez répliquer des objets vers un compartiment de destination unique ou plusieurs compartiments de destination. Les compartiments de destination peuvent se trouver dans une région différente Régions AWS ou dans la même région que le compartiment source.

Il existe deux types de réplication : la réplication en direct et la réplication à la demande.

- Réplication en direct : pour répliquer automatiquement les objets nouveaux et mis à jour à mesure qu'ils sont enregistrés dans le compartiment source, utilisez la réplication en direct. La réplication en direct ne réplique pas les objets qui existaient dans le compartiment avant la configuration de la réplication. Pour répliquer des objets qui existaient avant la configuration de la réplication, utilisez la réplication à la demande.

- Réplication à la demande : pour répliquer des objets existants depuis le compartiment source vers un ou plusieurs compartiments de destination à la demande, utilisez la réplication par lot S3. Pour en savoir plus sur la réplication d'objets existants, consultez Quand utiliser la réplication par lot S3.

Il existe deux formes de réplication en direct : la réplication interrégionale (CRR) et la réplication sur une même région (SRR).

- Réplication entre régions (CRR) : vous pouvez utiliser la CRR pour répliquer des objets dans différents compartiments Amazon S3. Régions AWS Pour plus d'informations sur la réplication CRR, consultez the section called "Quand utiliser la réplication entre Régions".
- Réplication sur une même région (SRR) : la réplication SRR permet de copier des objets entre des compartiments Amazon S3 d'une même Région AWS. Pour plus d'informations sur la réplication SRR, consultez the section called "Quand utiliser la réplication au sein d'une même Région".

Rubriques

- Pourquoi utiliser la réplication ?
- Quand utiliser la réplication entre Régions
- Quand utiliser la réplication au sein d'une même Région
- Quand utiliser la réplication à double sens (réplication bi-directionnelle)
- Quand utiliser la réplication par lot S3
- Exigences relatives à la charge de travail et réplication en direct
- Ce qui est répliqué par Amazon S3
- Exigences et considérations relatives à la réplication
- Présentation de la configuration de la réplication en direct
- Gestion ou suspension de la réplication en direct
- Réplication d'objets existants via la réplication par lot
- Résolution des problèmes de réplication
- Surveillance de la réplication avec des métriques, des notifications d'événements et des statuts

Pourquoi utiliser la réplication ?

La réplication entre Régions peut vous aider à réaliser les tâches suivantes :

- Répliquer des objets tout en conservant les métadonnées : vous pouvez utiliser la réplication pour créer des copies de vos objets qui conservent toutes les métadonnées, telles que l'heure de création et la version IDs d'origine des objets. Cette fonctionnalité est importante si vous devez vous assurer que votre réplica est identique à l'objet source.
- Répliquer des objets dans différentes classes de stockage – Vous pouvez utiliser la réplication pour placer directement des objets dans S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive ou une autre classe dans les compartiments de destination. Vous pouvez également répliquer vos données dans la même classe de stockage et utiliser des configurations de cycle de vie sur les compartiments de destination pour déplacer vos objets vers une classe de stockage à froid si leur ancienneté le justifie.
- Conservez des copies d'objets appartenant à des propriétaires différents : quel que soit le propriétaire de l'objet source, vous pouvez demander à Amazon S3 de transférer le propriétaire de la Compte AWS réplique au propriétaire du compartiment de destination. Il s'agit de l'option de substitution du propriétaire. Vous pouvez utiliser cette option pour limiter l'accès aux réplicas d'objets.
- Stockez les objets sur plusieurs sites Régions AWS : pour garantir les différences géographiques quant à l'emplacement de conservation de vos données, vous pouvez définir plusieurs compartiments de destination dans différents Régions AWS domaines. Cette fonctionnalité peut vous aider à répondre à certaines exigences de conformité.
- Répliquer des objets en 15 minutes : pour répliquer vos données dans la même région Région AWS ou entre différentes régions dans un délai prévisible, vous pouvez utiliser S3 Replication Time Control (S3 RTC). Le contrôle du délai de réplication S3 permet de répliquer 99,99 % des nouveaux objets stockés dans Simple Storage Service (Amazon S3) dans les 15 minutes (conformément à un contrat de niveau de service (SLA)). Pour de plus amples informations, veuillez consulter the section called "Utiliser le contrôle du délai de réplication S3".

  > **Note**
  >
  > Le contrôle du délai de réplication S3 ne s'applique pas à la réplication par lot. La réplication par lot est une tâche de réplication à la demande et peut être suivie avec les opérations par lot S3. Pour de plus amples informations, veuillez consulter Suivi de l'état de la tâche et des rapports de fin de tâche.

- Synchroniser des compartiments, répliquer des objets existants et répliquer des objets précédemment défaillants ou répliqués – Pour synchroniser des compartiments et répliquer des objets existants, utilisez la réplication par lot comme action de réplication à la demande. Pour plus

d'informations sur les conditions d'utilisation de la réplication par lot, consultez Quand utiliser la réplication par lot S3.

- Répliquer des objets et basculer vers un compartiment dans une autre Région AWS : pour que toutes les métadonnées et tous les objets restent synchronisés entre les compartiments pendant la réplication des données, utilisez des règles de réplication bidirectionnelle avant de configurer les contrôles de basculement du point d'accès multi-régions d'Amazon S3. Les règles de réplication bidirectionnelle permettent de s'assurer que lorsque des données sont écrites dans le compartiment S3 vers lequel le trafic bascule, ces données sont ensuite répliquées vers le compartiment source.

Quand utiliser la réplication entre Régions

La réplication entre Régions (CRR) S3 permet de copier des objets entre des compartiments Amazon S3 situés dans différentes Régions AWS. La réplication entre Régions aide à :

- Respecter les exigences de conformité – Bien que Simple Storage Service (Amazon S3) stocke vos données dans plusieurs zones de disponibilité distantes géographiquement par défaut, les exigences de conformité peuvent vous obliger à stocker les données séparées par des distances encore plus importantes. Pour satisfaire à ces exigences, la réplication entre Régions vous permet de répliquer des données entre des Régions AWS distantes.
- Minimiser le temps de latence — Si vos clients se trouvent dans deux zones géographiques, vous pouvez minimiser le temps de latence lors de l'accès aux objets en Régions AWS conservant des copies d'objets plus proches géographiquement de vos utilisateurs.
- Améliorez l'efficacité opérationnelle : si vous avez des clusters de calcul répartis dans deux régions différentes Régions AWS qui analysent le même ensemble d'objets, vous pouvez choisir de conserver des copies d'objets dans ces régions.

Quand utiliser la réplication au sein d'une même Région

La réplication dans une même Région (SRR) est utilisée pour copier des objets entre compartiments Amazon S3 d'une même Région AWS. La SRR vous aide à :

- Regrouper les journaux dans un même compartiment – Si vous stockez des journaux dans plusieurs compartiments ou sur différents comptes, vous pouvez facilement répliquer les journaux

dans un même compartiment d'une Région. Cela permet de simplifier le traitement des journaux dans un seul
emplacement.

- Configurer la réplication en direct entre les comptes de production et de test – Si vous, ou vos clients, disposez de comptes de production et de test qui utilisent les mêmes données, vous pouvez répliquer des objets entre différents comptes, tout en conservant les métadonnées d'objet.
- Respectez les lois sur la souveraineté des données — Vous pourriez être amené à stocker plusieurs copies de vos données séparément au Comptes AWS sein d'une région donnée. La réplication dans une même Région peut vous aider à répliquer des données critiques lorsque les exigences de conformité n'autorisent pas que les données sortent de votre
pays.

Quand utiliser la réplication à double sens (réplication bi-directionnelle)

- Créez des ensembles de données partagés sur plusieurs Régions AWS : grâce à la synchronisation des modifications des répliques, vous pouvez facilement répliquer les modifications de métadonnées, telles que les listes de contrôle d'accès aux objets (ACLs), les balises d'objets ou les verrous d'objets, sur les objets de réplication. Cette réplication bidirectionnelle est importante si vous voulez que tous les objets et les modifications des métadonnées des objets soient synchronisés. Vous pouvez activer la synchronisation de modification de réplica sur une règle de réplication nouvelle ou existante lors de l'exécution d'une réplication bidirectionnelle entre deux ou plusieurs compartiments dans des Régions AWS identiques ou différentes.
- Maintenez les données synchronisées entre les régions pendant le basculement : vous pouvez synchroniser les données dans des compartiments entre elles en Régions AWS configurant des règles de réplication bidirectionnelle avec la réplication inter-régions (CRR) S3 directement à partir d'un point d'accès multirégional. Pour prendre une décision éclairée quant au moment de lancer le basculement, vous pouvez également activer les métriques de réplication S3 afin de pouvoir surveiller la réplication dans Amazon CloudWatch, dans S3 Replication Time Control (S3 RTC) ou depuis le point d'accès multirégional.
- Make your application highly available (Rendre votre application hautement disponible) : même en cas de perturbation du trafic régional, vous pouvez utiliser des règles de réplication bidirectionnelle pour que toutes les métadonnées et tous les objets restent synchronisés entre les compartiments pendant la réplication des données.

Quand utiliser la réplication par lot S3

La réplication par lot réplique des objets existants dans différents compartiments (option à la demande). Contrairement à la réplication en direct, ces tâches peuvent être exécutées selon les besoins. La réplication par lot peut vous aider à réaliser les tâches suivantes :

- Répliquer des objets existants – Vous pouvez utiliser la réplication par lot pour répliquer des objets qui ont été ajoutés au compartiment avant la configuration de la réplication dans une même région ou de la réplication entre Régions.
- Répliquer les objets qui n'ont pas pu être répliqués auparavant – Vous pouvez filtrer une tâche de réplication par lot pour tenter de répliquer des objets dont le statut de réplication a ÉCHOUÉ.
- Répliquer des objets déjà répliqués – Vous pourriez devoir stocker plusieurs copies de vos données dans des Comptes AWS ou des Régions AWS distincts. La réplication par lot peut répliquer des objets existants vers des destinations nouvellement ajoutées.
- Répliquer des réplicas d'objets créés à partir d'une règle de réplication – Les configurations de réplication créent des réplicas d'objets dans des compartiments de destination. Les réplicas d'objets peuvent être répliqués uniquement via la réplication par lot.

Exigences relatives à la charge de travail et réplication en direct

Selon les exigences de votre charge de travail, certains types de réplication en direct seront mieux adaptés à votre cas d'utilisation que d'autres. Utilisez le tableau suivant pour déterminer le type de réplication à utiliser dans votre situation et si vous devez utiliser le contrôle du temps de réplication S3 (S3 RTC) pour votre charge de travail. Le contrôle du temps de réplication S3 permet de répliquer 99,99 % des nouveaux objets stockés dans Amazon S3 dans les 15 minutes (conformément à un contrat de niveau de service (SLA)). Pour de plus amples informations, veuillez consulter the section called "Utiliser le contrôle du délai de réplication S3".

Exigence relative à la charge de travail	S3 RTC (SLA de 15 minutes)	Réplication entre régions (CRR)	Réplication sur une même région (SRR)
Répliquer des objets entre différents Comptes AWS	Oui	Oui	Oui
Répliquez des objets au même endroit dans	Non	Non	Oui

Exigence relative à la charge de travail	S3 RTC (SLA de 15 minutes)	Réplication entre régions (CRR)	Réplication sur une même région (SRR)
Région AWS un délai de 24 à 48 heures (sans respecter les SLA)			
Répliquez des objets entre différents Régions AWS dans un délai de 24 à 48 heures (non garanti par un SLA)	Non	Oui	Non
Temps de réplication prévisible : défini par un SLA pour répliquer 99,9 % des objets en 15 minutes	Oui	Non	Non

Ce qui est répliqué par Amazon S3

Dans les compartiments, Simple Storage Service (Amazon S3) réplique uniquement les éléments spécifiques qui sont configurés pour la réplication.

Rubriques

- Qu'est-ce qui est répliqué avec les configurations de réplication ?
- Qu'est-ce qui n'est pas répliqué avec les configurations de réplication ?

Qu'est-ce qui est répliqué avec les configurations de réplication ?

Par défaut, Simple Storage Service (Amazon S3) réplique les éléments suivants :

- Objets créés après l'ajout d'une configuration de réplication.
- Objets non chiffrés.

- Objets chiffrés à l'aide de clés fournies par le client (SSE-C), objets chiffrés au repos sous une clé gérée Amazon S3 (SSE-S3) ou une clé KMS stockée dans AWS Key Management Service (SSE-KMS). Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets chiffrés".
- Métadonnées d'objet des objets source vers les réplicas. Pour plus d'informations sur la réplique des métadonnées des réplicas vers les objets source, consultez Réplication des modifications des métadonnées avec la synchronisation des modifications de réplica.
- Uniquement les objets du compartiment source pour lesquels le propriétaire du compartiment est autorisé à lire les objets et les listes de contrôle d'accès (ACLs).

  Pour de plus informations sur la propriété des ressources, consultez Propriété du compartiment et de l'objet Amazon S3.
- Les mises à jour des listes ACL d'objet, sauf si vous indiquez à Amazon S3 de modifier le propriétaire des réplicas lorsque les compartiments source et de destination n'appartiennent pas aux mêmes comptes.

  Pour de plus amples informations, veuillez consulter Modification du propriétaire d'un réplica.

  Cela peut prendre un certain temps avant qu'Amazon S3 puisse synchroniser ACLs les deux. Ce changement de propriété s'applique uniquement aux objets créés après l'ajout d'une configuration de réplication dans le compartiment.
- Les balises d'objets, le cas échéant.
- Les informations de conservation du verrouillage des objets S3, le cas échéant.

  Quand Amazon S3 réplique des objets pour lesquels des informations de conservation ont été appliquées, il applique ces mêmes contrôles de conservation à vos réplicas, remplaçant ainsi la période de conservation par défaut configurée sur vos compartiments de destination. Si vous n'avez pas de contrôles de conservation appliqués aux objets de votre compartiment source, et que vous répliquez dans un compartiment de destination dont la période de conservation par défaut est définie, la période de conservation par défaut du compartiment de destination est appliquée à vos répliques d'objets. Pour plus d'informations, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

Impact des opérations de suppression sur la réplication

Si vous supprimez un objet du compartiment source, les actions suivantes se produisent par défaut :

- Si vous émettez une demande de suppression (DELETE) sans spécifier d'ID de version d'objet, Amazon S3 ajoute un marqueur de suppression. Amazon S3 traite le marqueur de suppression comme suit :
  - Si vous utilisez la dernière version de la configuration de réplication, en spécifiant l'élément `Filter` dans une règle de configuration de réplication, Simple Storage Service (Amazon S3) ne réplique pas le marqueur de suppression par défaut. Vous pouvez toutefois ajouter la réplication des marqueurs de suppression aux non-tag-based règles. Pour de plus amples informations, veuillez consulter Répliquer des marqueurs de suppression entre les compartiments.
  - Si vous ne spécifiez pas l'élément `Filter`, Simple Storage Service (Amazon S3) suppose que la configuration de réplication est la version V1 et réplique les marqueurs de suppression résultant des actions de l'utilisateur. Toutefois, si Amazon S3 supprime un objet en raison d'une action de cycle de vie, le marqueur de suppression n'est pas répliqué dans les compartiments de destination.
- Si vous spécifiez un ID de version d'objet à supprimer dans une requête `DELETE`, Amazon S3 supprime cette version de l'objet dans le compartiment source. Mais le service ne réplique pas la suppression dans les compartiments de destination. En d'autres termes, il ne supprime pas la même version de l'objet dans les compartiments de destination. Les données sont ainsi protégées contre les suppressions malveillantes.

Qu'est-ce qui n'est pas répliqué avec les configurations de réplication ?

Par défaut, Simple Storage Service (Amazon S3) ne réplique pas les éléments suivants :

- Les objets du compartiment source qui sont des réplicas ayant été créés par une autre règle de réplication. Supposons, par exemple, que vous configurez une réplication où le compartiment A est le compartiment source et le compartiment B celui de destination. Supposons ensuite que vous ajoutez une autre configuration de réplication où le compartiment B est le compartiment source et le compartiment C celui de destination. Dans ce cas, les objets du compartiment B qui sont les réplicas d'objets du compartiment A ne sont pas répliqués dans le compartiment C.

  Pour répliquer des objets qui sont des réplicas, utilisez la réplication par lot. Pour en savoir plus sur la configuration de la réplication par lot, consultez Réplication d'objets existants.
- Objets du compartiment source qui ont déjà été répliqués vers une autre destination. Par exemple, si vous changez le compartiment de destination dans une configuration de réplication existante, Simple Storage Service (Amazon S3) ne procède pas à une nouvelle réplication des objets.

Pour répliquer des objets précédemment répliqués, utilisez la réplication par lot. Pour en savoir plus sur la configuration de la réplication par lot, consultez Réplication d'objets existants.

- La réplication par lot ne prend pas en charge la réplication répétée d'objets qui ont été supprimés avec l'ID de version de l'objet dans le compartiment de destination. Pour répéter la réplication de ces objets, vous pouvez copier les objets sources en place avec une tâche de copie par lot. La copie de ces objets en place crée de nouvelles versions des objets dans le compartiment source et lance automatiquement la réplication vers la destination. Pour plus d'informations sur l'utilisation de Batch Copy, consultez Exemples qui utilisent des opérations par lot pour copier des objets.
- Par défaut, lors de la réplication à partir d'un autre compartiment Compte AWS, les marqueurs de suppression ajoutés au compartiment source ne sont pas répliqués.

  Pour savoir comment répliquer des marqueurs de suppression, consultez Répliquer des marqueurs de suppression entre les compartiments.
- Objets stockés dans les classes ou niveaux de stockage S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive, Archive Access de S3 Intelligent-Tiering ou Deep Archive Access de S3 Intelligent-Tiering. Vous ne pouvez pas répliquer ces objets tant que vous ne les avez pas restaurés et copiés dans une autre classe de stockage.

  Pour en savoir plus sur S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive, consultez Classes de stockage pour les objets rarement consultés.

  Pour en savoir plus sur S3 Intelligent-Tiering, consultez Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering.
- Objets dans le compartiment source pour lesquels le propriétaire du compartiment ne dispose pas des autorisations de réplication suffisantes.

  Pour obtenir des informations sur la façon dont un propriétaire d'objet peut accorder des autorisations à un propriétaire de compartiment, consultez Octroi d'autorisations intercomptes pour charger des objets tout en garantissant que le propriétaire du compartiment dispose d'un contrôle total.
- Les mises à jour des sous-ressources de niveau compartiment.

  Par exemple, si vous modifiez la configuration du cycle de vie ou ajoutez une configuration de notification à votre compartiment source, ces modifications ne sont pas appliquées au compartiment de destination. Cette fonction permet ainsi d'avoir des configurations différentes dans les compartiments source et de destination.

- Actions effectuées par la configuration du cycle de vie.

  Par exemple, si la configuration du cycle de vie est activée uniquement sur votre compartiment source, Simple Storage Service (Amazon S3) crée des marqueurs de suppression pour les objets expirés, mais ne réplique pas ces marqueurs. Si vous souhaitez appliquer la même configuration de cycle de vie aux compartiments source et de destination, activez la même configuration de cycle de vie sur les deux. Pour en savoir plus sur la configuration du cycle de vie, consultez Gestion du cycle de vie des objets.
- Lorsque vous utilisez des règles de réplication basées sur des balises avec la réplication en direct, les nouveaux objets doivent être balisés avec la balise de règle de réplication correspondante dans l'opération `PutObject`. Dans le cas contraire, les objets ne sont pas répliqués. Si des objets sont balisés après l'opération `PutObject`, ils ne sont pas non plus répliqués.

  Pour répliquer des objets balisés après l'opération `PutObject`, vous devez utiliser la réplication par lot S3. Pour en savoir plus sur la réplication par lot, consultez Réplication d'objets existants.

Exigences et considérations relatives à la réplication

La réplication Amazon S3 exige de respecter les conditions suivantes :

- Le propriétaire du compartiment source doit avoir Régions AWS activé la source et la destination pour son compte. Le propriétaire du compartiment de destination doit avoir activé la Région de destination pour son compte.

  Pour plus d'informations sur l'activation ou la désactivation d'un Région AWS, voir Spécifier le compte que Régions AWS votre compte peut utiliser dans le Guide de Gestion de compte AWS référence.
- La gestion des versions doit être activée pour les compartiments source et de destination. Pour plus d'informations sur la gestion des versions, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.
- Simple Storage Service (Amazon S3) doit disposer des autorisations adéquates pour répliquer en votre nom les objets issus du compartiment source vers le ou les compartiments de destination. Pour plus d'informations sur ces autorisations, consultez Configuration des autorisations pour la réplication en direct.
- Si le propriétaire du compartiment source ne possède pas l'objet dans le compartiment, le propriétaire de l'objet doit accorder au propriétaire du compartiment les autorisations `READ` et

`READ_ACP` avec la liste de contrôle d'accès (ACL) de l'objet. Pour plus d'informations, consultez Présentation de la liste de contrôle d'accès (ACL).

- Si le verrouillage des objets S3 est activé dans le compartiment source, alors il doit également l'être dans les compartiments de destination.

  Pour activer la réplication sur un bucket sur lequel Object Lock est activé, vous devez utiliser l' AWS Command Line Interface API REST ou AWS SDKs. Pour plus d'informations générales, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

  > **Note**
  >
  > Vous devez accorder deux nouvelles autorisations sur le compartiment S3 source dans le rôle AWS Identity and Access Management (IAM) que vous utilisez pour configurer la réplication. Les deux nouvelles autorisations sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d'une autorisation `s3:Get*`, il répond aux exigences. Pour plus d'informations, consultez Configuration des autorisations pour la réplication en direct.

Pour plus d'informations, consultez Présentation de la configuration de la réplication en direct.

Si vous définissez la configuration de réplication dans un scénario à plusieurs comptes, où les compartiments source et de destination appartiennent à différents Comptes AWS, la condition supplémentaire suivante s'applique :

- Le propriétaire des compartiments de destination doit accorder des autorisations au propriétaire du compartiment source lui permettant de répliquer des objets avec une politique de compartiment. Pour plus d'informations, consultez Octroi d'autorisations lorsque les compartiments source et de destination appartiennent à des entités différentes Comptes AWS.
- Les compartiments de destination ne peuvent pas être configurés en tant que compartiment Paiement par le demandeur. Pour de plus amples informations, veuillez consulter Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation.

Considérations liées à la réplication

Avant de créer une configuration de réplication, tenez compte des considérations suivantes.

Rubriques

- Configuration de cycle de vie et réplicas d'objets
- Configuration de la gestion des versions et configuration de la réplication
- Utiliser la réplication S3 avec S3 Intelligent-Tiering
- Configuration de la journalisation et configuration de la réplication
- Réplication entre Régions et Région de destination
- Réplication par lot S3
- Contrôle du temps de réplication S3

Configuration de cycle de vie et réplicas d'objets

Le temps nécessaire à Amazon S3 pour répliquer un objet dépend de la taille de ce dernier. Pour les objets volumineux, cela peut prendre plusieurs heures. Même si la mise à disposition d'un réplica dans la destination peut prendre du temps, la création du réplica prend autant de temps que la création de l'objet correspondant dans le compartiment source. Si une configuration de cycle de vie est activée dans le compartiment de destination, les règles de cycle de vie tiennent compte du moment de création de l'objet à l'origine, et non pas du moment où le réplica est devenu disponible dans le compartiment de destination.

La configuration de réplication nécessite que le compartiment soit activé pour la gestion des versions. Lorsque vous activez la gestion des versions pour un compartiment, considérez les éléments suivants :

- Si vous avez une configuration de cycle de vie d'expiration des objets, après avoir activé la gestion des versions, ajoutez une stratégie `NonCurrentVersionExpiration` pour conserver le même comportement de suppression définitive que celui défini avant l'activation de la gestion des versions.
- Si vous avez une configuration de cycle de vie de transition, après avoir activé la gestion des versions, envisagez d'ajouter une politique `NonCurrentVersionTransition`.

Configuration de la gestion des versions et configuration de la réplication

La gestion des versions doit être activée pour les deux compartiments source et de destination lorsque vous configurez une réplication dans un compartiment. Après avoir activé la gestion des versions dans les compartiments source et de destination, et configuré la réplication dans le compartiment source, les problèmes suivants se produisent :

- Si vous tentez de désactiver la gestion des versions sur le compartiment source, Amazon S3 renvoie une erreur. Vous devez supprimer la configuration de réplication avant de désactiver la gestion des versions dans le compartiment source.
- Si vous désactivez la gestion des versions dans le compartiment de destination, la réplication échoue. L'objet source a le statut de réplication `FAILED`.

Utiliser la réplication S3 avec S3 Intelligent-Tiering

La classe de stockage S3 Intelligent-Tiering est conçue pour optimiser les coûts de stockage en transférant automatiquement les données vers le niveau d'accès le plus économique. Moyennant des frais mensuels minimes de surveillance et d'automatisation des objets, S3 Intelligent-Tiering surveille les modèles d'accès et déplace automatiquement les objets qui n'ont pas été consultés vers des niveaux d'accès moins coûteux.

La réplication d'objets stockés dans S3 Intelligent-Tiering avec la réplication par lot S3 ou l'invocation de CopyObject ou de UploadPartCopy constitue un accès. Dans ces cas, les objets source des opérations de copie ou de réplication sont hiérarchisés.

Pour plus d'informations sur S3 Intelligent-Tiering, consultez Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering.

Configuration de la journalisation et configuration de la réplication

Si Amazon S3 livre des journaux à un compartiment où la réplication est activée, il réplique les objets journaux.

Si les journaux d'accès au serveur ou les journaux AWS CloudTrail sont activés sur votre compartiment source ou de destination, Amazon S3 inclut les demandes liées à la réplication dans ces journaux. Par exemple, Amazon S3 consigne chaque objet qu'il réplique.

Réplication entre Régions et Région de destination

Amazon S3 Cross-Region Replication (CRR) est utilisé pour copier des objets dans différents compartiments S3. Régions AWS Vous pouvez choisir la Région de votre compartiment de destination en fonction de vos besoins professionnels ou de considérations tarifaires. Par exemple, les frais de transfert de données entre Régions varient en fonction des Régions que vous choisissez.

Supposons que vous avez choisi USA Est (Virginie du Nord) (`us-east-1`) comme région pour votre compartiment source. Si vous choisissez USA Ouest (Oregon) (`us-west-2`) comme région pour vos

compartiments de destination, vous payez plus que si vous choisissez la région USA Est (Ohio) (`us-east-2`). Pour en savoir plus sur la tarification, consultez « Tarification du transfert de données » dans Tarification Amazon S3.

Aucun frais de transfert de données n'est associé à la réplication dans une même Région (SRR).

Réplication par lot S3

Pour obtenir des informations sur les considérations relatives à la réplication par lot, consultez Considérations sur la réplication par lot S3.

Contrôle du temps de réplication S3

Pour obtenir des informations sur les bonnes pratiques et les considérations relatives au contrôle du temps de réplication S3 (S3 RTC), consultez Bonnes pratiques et directives de contrôle du délai de réplication S3.

Présentation de la configuration de la réplication en direct

> **Note**
>
> Les objets qui existaient avant la configuration de la réplication ne sont pas répliqués automatiquement. En d'autres termes, Simple Storage Service (Amazon S3) ne réplique pas les objets de manière rétroactive. Pour répliquer des objets créés avant la configuration de la réplication, utilisez la réplication par lot S3. Pour plus d'informations sur la configuration de la réplication par lot, consultez Réplication d'objets existants.

Pour activer la réplication en direct (réplication sur une même région (SRR) ou réplication interrégionale (CRR)), ajoutez une configuration de réplication à votre compartiment source. Cette configuration indique à Amazon S3 de répliquer les objets comme spécifié. Dans la configuration de réplication, vous devez renseigner les éléments suivants :

- Compartiments de destination – Compartiments dans lesquels vous souhaitez qu'Simple Storage Service (Amazon S3) réplique les objets.
- Objets que vous voulez répliquer : vous pouvez répliquer tous les objets figurant dans le compartiment source ou un sous-ensemble d'objets. Vous identifiez un sous-ensemble en fournissant un préfixe de nom de clé, une ou plusieurs balises d'objets, ou les deux dans la configuration.

Par exemple, si vous configurez une règle de réplication pour ne répliquer que les objets dotés du préfixe de nom de clé `Tax/`, Amazon S3 réplique les objets avec les clés `Tax/doc1` et `Tax/doc2`. Mais le service ne réplique pas les objets dotés d'une clé `Legal/doc3`. Si vous spécifiez un préfixe et une ou plusieurs balises, Simple Storage Service (Amazon S3) réplique uniquement les objets dotés du préfixe de clé et des balises spécifiques.

- Un rôle AWS Identity and Access Management (IAM) : Amazon S3 assume ce rôle IAM pour répliquer des objets en votre nom. Pour plus d'informations sur la création de ce rôle IAM et la gestion des autorisations, consultez Configuration des autorisations pour la réplication en direct.

Outre ces conditions minimales requises, vous pouvez choisir les options suivantes :

- Classe de stockage des réplicas – Par défaut, Simple Storage Service (Amazon S3) stocke les réplicas d'objet dans la même classe de stockage que celle de l'objet source. Vous pouvez spécifier une classe de stockage différente pour les réplicas.
- Propriété des réplicas – Simple Storage Service (Amazon S3) suppose qu'un réplica d'objet appartient toujours au propriétaire de l'objet source. Ainsi, lorsqu'il réplique des objets, il réplique également la liste de contrôle d'accès (ACL) correspondante ou le paramètre de propriété de l'objet S3. Si les compartiments source et de destination appartiennent à des Comptes AWS différents, vous pouvez configurer la réplication de sorte à remplacer le propriétaire d'un réplica par le Compte AWS qui possède le compartiment de destination. Pour de plus amples informations, veuillez consulter the section called "Modification du propriétaire d'un réplica".

Vous pouvez configurer la réplication à l'aide de la console Amazon S3 AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs Pour obtenir des instructions détaillées sur la configuration de la réplication, consultez the section called "Procédures de réplication".

Amazon S3 fournit également les opérations d'API REST pour prendre en charge la configuration des règles de réplication. Pour plus d'informations, consultez les rubriques suivantes dans la Référence d'API Amazon Simple Storage Service :

- PutBucketReplication
- GetBucketReplication
- DeleteBucketReplication

Rubriques

- Éléments du fichier de configuration de réplication
- Configuration des autorisations pour la réplication en direct
- Exemples de configuration de la réplication en direct

Éléments du fichier de configuration de réplication

Amazon S3 stocke une configuration de réplication au format XML. Si vous configurez la réplication par programmation via l'API REST Amazon S3, vous spécifiez les différents éléments de votre configuration de réplication dans ce fichier XML. Si vous configurez la réplication via l' AWS Command Line Interface (AWS CLI), vous spécifiez votre configuration de réplication au format JSON. Pour des exemples JSON, consultez les procédures dans the section called "Procédures de réplication".

> **Note**
>
> La dernière version du format XML de configuration de réplication est V2. Les configurations de réplication XML V2 sont celles qui contiennent l'élément `<Filter>` pour les règles et les règles qui spécifient le contrôle du délai de réplication S3.
> Pour afficher votre version de configuration de réplication, vous pouvez utiliser l'opération d'API `GetBucketReplication`. Pour plus d'informations, consultez GetBucketReplication dans la Référence d'API Amazon Simple Storage Service.
> Pour assurer la rétrocompatibilité, Amazon S3 continue de prendre en charge le format de configuration de réplication XML V1. Si vous avez utilisé le format de configuration de réplication XML V1, consultez Considérations relatives à la rétrocompatibilité pour les considérations de rétrocompatibilité.

Dans le fichier XML de configuration de réplication, vous devez spécifier un rôle AWS Identity and Access Management (IAM) et une ou plusieurs règles, comme illustré dans l'exemple suivant :

```
<ReplicationConfiguration>
    <Role>IAM-role-ARN</Role>
    <Rule>
        ...
    </Rule>
    <Rule>
```

```
        ...
    </Rule>
     ...
</ReplicationConfiguration>
```

Amazon S3 ne peut pas répliquer d'objets sans votre autorisation. Vous accordez des autorisations à Amazon S3 avec le rôle IAM que vous spécifiez dans la configuration de réplication. Amazon S3 endosse ce rôle IAM pour répliquer des objets en votre nom. Vous devez accorder les autorisations requises au rôle IAM en premier. Pour plus d'informations sur la gestion des autorisations, consultez Configuration des autorisations pour la réplication en direct.

Vous ajoutez une seule règle dans la configuration de réplication pour les scénarios suivants :

- Vous souhaitez répliquer tous les objets.
- Vous souhaitez répliquer un seul sous-ensemble d'objets. Vous identifiez le sous-ensemble d'objets en ajoutant un filtre dans la règle. Dans le filtre, vous spécifiez un préfixe de clé d'objet et/ou des balises pour identifier le sous-ensemble d'objets auquel la règle s'applique. Les filtres ciblent les objets qui correspondent exactement aux valeurs que vous avez spécifiées.

Si vous souhaitez répliquer des sous-ensembles d'objets différents, vous ajoutez plusieurs règles dans une configuration de réplication. Dans chaque règle, vous spécifiez un filtre qui sélectionne un sous-ensemble différent. Par exemple, vous pouvez choisir de répliquer des objets qui possèdent les préfixes de clé `tax/` ou `document/`. Pour ce faire, vous ajoutez deux règles, l'une qui spécifie le filtre de préfixe de clé `tax/` et l'autre qui spécifie le préfixe de clé `document/`. Pour plus d'informations sur les préfixes de clé d'objet, consultez Organisation des objets à l'aide de préfixes.

Les sections suivantes fournissent des informations supplémentaires.

Rubriques

- Configuration de base d'une règle
- Facultatif : Spécification d'un filtre
- Configurations de destinations supplémentaires
- Exemples de configuration de réplication
- Considérations relatives à la rétrocompatibilité

Configuration de base d'une règle

Chaque règle doit inclure le statut et la priorité de la règle. La règle doit également indiquer s'il faut répliquer les marqueurs de suppression.

- L'élément `<Status>` indique si la règle est activée ou désactivée en utilisant les valeurs `Enabled` ou `Disabled`. Si une règle est désactivée, Simple Storage Service (Amazon S3) n'effectue pas les actions spécifiées dans la règle.
- L'élément `<Priority>` indique quelle règle a priorité en cas de conflit de deux règles de réplication ou plus. Simple Storage Service (Amazon S3) tente de répliquer les objets selon toutes les règles de réplication. Toutefois, s'il existe deux règles ou plus avec le même compartiment de destination, les objets sont répliqués selon la règle avec la priorité la plus élevée. Plus le nombre est élevé, plus la priorité est haute.
- L'élément `<DeleteMarkerReplication>` indique s'il faut répliquer les marqueurs de suppression en utilisant les valeurs `Enabled` ou `Disabled`.

Dans la configuration de l'élément `<Destination>`, vous devez fournir le nom du ou des compartiments de destination où vous voulez qu'Amazon S3 réplique les objets.

L'exemple suivant indique les conditions minimales requises pour une règle V2. Pour assurer la compatibilité descendante, Amazon S3 continue de prendre en charge le format XML V1. Pour plus d'informations, consultez Considérations relatives à la rétrocompatibilité.

```
...
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled-or-Disabled</Status>
        <Filter>
            <Prefix></Prefix>
        </Filter>
        <Priority>integer</Priority>
        <DeleteMarkerReplication>
           <Status>Enabled-or-Disabled</Status>
        </DeleteMarkerReplication>
        <Destination>
           <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
        </Destination>
    </Rule>
    <Rule>
         ...
    </Rule>
     ...
```

```
...
```

Vous pouvez également spécifier d'autres options de configuration. Par exemple, vous pouvez choisir d'utiliser une classe de stockage pour les réplicas d'objets qui diffèrent de la classe associée à l'objet source.

Facultatif : Spécification d'un filtre

Pour choisir un sous-ensemble d'objets auquel la règle s'applique, ajoutez un filtre facultatif. Vous pouvez filtrer par préfixe de clé d'objet et/ou par balises d'objets. Si vous filtrez par préfixe de clé et par balises d'objet, Amazon S3 combine ces filtres au moyen de l'opérateur logique `AND`. En d'autres termes, la règle s'applique à un sous-ensemble d'objets doté à la fois d'un préfixe de clé et de balises spécifiques.

Filtre basé sur un préfixe de clé d'objet

Pour spécifier une règle avec un filtre basé sur un préfixe de clé d'objet, utilisez le code XML suivant. Vous ne pouvez spécifier qu'un seul préfixe par règle.

```
<Rule>
    ...
    <Filter>
        <Prefix>key-prefix</Prefix>
    </Filter>
    ...
</Rule>
...
```

Filtre basé sur des balises d'objet

Pour spécifier une règle avec un filtre basé sur des balises d'objets, utilisez le code XML suivant. Vous pouvez spécifier une ou plusieurs balises d'objets.

```
<Rule>
    ...
    <Filter>
        <And>
            <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
            </Tag>
```

```
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
        </And>
    </Filter>
    ...
</Rule>
...
```

Filtre basé sur un préfixe de clé et des balises d'objet

Pour spécifier un filtre de règle combinant un préfixe de clé et des balises d'objets, utilisez le code XML suivant. Vous enveloppez ces filtres dans un élément parent <And>. Amazon S3 effectue une opération logique AND pour combiner ces filtres. En d'autres termes, la règle s'applique à un sous-ensemble d'objets doté à la fois d'un préfixe de clé et de balises spécifiques.

```
<Rule>
    ...
    <Filter>
        <And>
            <Prefix>key-prefix</Prefix>
            <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
            </Tag>
            <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
            </Tag>
             ...
    </Filter>
    ...
</Rule>
...
```

> **Note**
>
> - Si vous spécifiez une règle avec un élément <Filter> vide, votre règle s'applique à tous les objets de votre compartiment.

- Lorsque vous utilisez des règles de réplication basées sur des balises avec la réplication en direct, les nouveaux objets doivent être balisés avec la balise de règle de réplication correspondante dans l'opération `PutObject`. Dans le cas contraire, les objets ne sont pas répliqués. Si des objets sont balisés après l'opération `PutObject`, ils ne sont pas non plus répliqués.

  Pour répliquer des objets balisés après l'opération `PutObject`, vous devez utiliser la réplication par lot S3. Pour en savoir plus sur la réplication par lot, consultez Réplication d'objets existants.

Configurations de destinations supplémentaires

Dans la configuration de destination, vous spécifiez le ou les compartiments dans lesquels vous voulez qu'Amazon S3 réplique les objets. Vous pouvez définir des configurations pour répliquer des objets d'un compartiment source dans un ou plusieurs compartiments de destination.

```
...
<Destination>
    <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
</Destination>
...
```

Vous pouvez ajouter les options suivantes dans l'élément `<Destination>` :

Rubriques

- Spécifier une classe de stockage
- Ajouter plusieurs compartiments de destination
- Spécifier des paramètres différents pour chaque règle de réplication avec plusieurs compartiments de destination
- Modification du propriétaire d'un réplica
- Activer le contrôle du délai de réplication S3
- Répliquez les objets créés avec le chiffrement côté serveur en utilisant AWS KMS

Spécifier une classe de stockage

Vous pouvez spécifier la classe de stockage pour les réplicas d'objets. Par défaut, Amazon S3 utilise la classe de stockage de l'objet source pour créer les réplicas d'objets, comme dans l'exemple ci-dessous.

```
...
<Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
</Destination>
...
```

Ajouter plusieurs compartiments de destination

Vous pouvez ajouter plusieurs compartiments de destination dans une configuration de réplication unique, comme suit.

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
    <ID>Rule-2</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled-or-Disabled</Status>
    </DeleteMarkerReplication>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
    </Destination>
</Rule>
...
```

Spécifier des paramètres différents pour chaque règle de réplication avec plusieurs compartiments de destination

Lorsque vous ajoutez plusieurs compartiments de destination dans une configuration de réplication unique, vous pouvez spécifier différents paramètres pour chaque règle de réplication, comme suit.

```
...
<Rule>
    <ID>Rule-1</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Disabled</Status>
    </DeleteMarkerReplication>
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket1</Bucket>
    </Destination>
</Rule>
<Rule>
    <ID>Rule-2</ID>
    <Status>Enabled-or-Disabled</Status>
    <Priority>integer</Priority>
    <DeleteMarkerReplication>
       <Status>Enabled</Status>
    </DeleteMarkerReplication>
      <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
```

```
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket2</Bucket>
    </Destination>
</Rule>
...
```

Modification du propriétaire d'un réplica

Lorsque les compartiments source et de destination ne sont pas détenus par les mêmes comptes, vous pouvez remplacer le propriétaire de la réplique par le Compte AWS propriétaire du compartiment de destination. Pour ce faire, ajoutez l'élément `<AccessControlTranslation>`. Cet élément prend la valeur `Destination`.

```
...
<Destination>
   <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
   <Account>destination-bucket-owner-account-id</Account>
   <AccessControlTranslation>
       <Owner>Destination</Owner>
   </AccessControlTranslation>
</Destination>
...
```

Si vous n'ajoutez pas l'`<AccessControlTranslation>`élément à la configuration de réplication, les répliques appartiennent au même propriétaire Compte AWS que l'objet source. Pour de plus amples informations, veuillez consulter Modification du propriétaire d'un réplica.

Activer le contrôle du délai de réplication S3

Vous pouvez activer le contrôle du délai de réplication S3 dans votre configuration de réplication. S3 RTC réplique la plupart des objets en quelques secondes et 99,99 % des objets en l'espace de 15 minutes (soutenu par un contrat de niveau de service (SLA)).

> **Note**
>
> Seule une valeur de `<Minutes>15</Minutes>` est acceptée pour les éléments `<EventThreshold>` et `<Time>`.

```
...
```

```
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <Metrics>
    <Status>Enabled</Status>
    <EventThreshold>
      <Minutes>15</Minutes>
    </EventThreshold>
  </Metrics>
  <ReplicationTime>
    <Status>Enabled</Status>
    <Time>
      <Minutes>15</Minutes>
    </Time>
  </ReplicationTime>
</Destination>
...
```

Pour de plus amples informations, veuillez consulter Satisfaction aux exigences de conformité à l'aide du contrôle du temps de réplication S3. Pour obtenir des exemples d'API, consultez PutBucketReplication dans la Référence des API Amazon Simple Storage Service.

Répliquez les objets créés avec le chiffrement côté serveur en utilisant AWS KMS

Votre compartiment source peut contenir des objets créés avec un chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS). Par défaut, Simple Storage Service (Amazon S3) ne réplique pas ces objets. Vous pouvez éventuellement demander à Simple Storage Service (Amazon S3) de répliquer ces objets. Pour ce faire, commencez par choisir explicitement cette fonctionnalité en ajoutant l'élément `<SourceSelectionCriteria>`. Indiquez ensuite le AWS KMS key (pour le compartiment Région AWS de destination) à utiliser pour chiffrer les répliques d'objets. Les exemples suivants montrent comment spécifier ces éléments.

```
...
<SourceSelectionCriteria>
  <SseKmsEncryptedObjects>
    <Status>Enabled</Status>
  </SseKmsEncryptedObjects>
</SourceSelectionCriteria>
<Destination>
  <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
  <EncryptionConfiguration>
    <ReplicaKmsKeyID>AWS KMS key ID to use for encrypting object replicas</
ReplicaKmsKeyID>
```

```
  </EncryptionConfiguration>
</Destination>
...
```

Pour plus d'informations, consultez Réplication d'objets chiffrés (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

Exemples de configuration de réplication

Pour commencer, vous pouvez ajouter les exemples de configuration de réplication suivants à votre compartiment, selon les besoins.

> **Important**
>
> Pour ajouter une configuration de réplication à un compartiment, vous devez disposer de l'autorisation `iam:PassRole`. Cette autorisation vous permet de transmettre le rôle IAM qui accorde les autorisations de réplication à Amazon S3. Vous spécifiez le rôle IAM en fournissant l'Amazon Resource Name (ARN) utilisé dans l'élément `<Role>` du fichier XML de la configuration de réplication. Pour plus d'informations, consultez Octroi d'autorisations à un utilisateur pour transférer un rôle à un Service AWS dans le Guide de l'utilisateur IAM.

Example 1 : Configuration de réplication à une seule règle

La configuration de réplication de base suivante indique une règle. Cette règle spécifie un rôle IAM qu'Simple Storage Service (Amazon S3) peut endosser et un compartiment de destination unique pour les réplicas d'objets. La valeur `Enabled` de l'élément `<Status>` indique que la règle est en vigueur.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>

    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Pour choisir un sous-ensemble d'objets à répliquer, vous pouvez ajouter un filtre. Dans la configuration suivante, le filtre spécifie un préfixe de clé d'objet. Cette règle s'applique aux objets dotés du préfixe *Tax/* dans leur nom de clé.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
       <Prefix>Tax/</Prefix>
    </Filter>

    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

Si vous spécifiez l'élément `<Filter>`, vous devez également inclure les éléments `<Priority>` et `<DeleteMarkerReplication>`. Dans cet exemple, la valeur que vous définissez pour l'élément `<Priority>` n'a aucune importance, car il existe une seule règle.

Dans la configuration suivante, le filtre spécifie un préfixe et deux balises. La règle s'applique au sous-ensemble d'objets dotés du préfixe de clé et des balises spécifiés. Notamment, elle s'applique aux objets dotés du préfixe *Tax/* dans leur nom de clé et des deux balises d'objets spécifiées. Dans cet exemple, la valeur que vous définissez pour l'élément `<Priority>` n'a aucune importance, car il existe une seule règle.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
```

```
        <Status>string</Status>
    </DeleteMarkerReplication>

    <Filter>
        <And>
          <Prefix>Tax/</Prefix>
          <Tag>
             <Tag>
                <Key>tagA</Key>
                <Value>valueA</Value>
             </Tag>
          </Tag>
          <Tag>
             <Tag>
                <Key>tagB</Key>
                <Value>valueB</Value>
             </Tag>
          </Tag>
       </And>

    </Filter>

    <Destination>
        <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

Vous pouvez spécifier une classe de stockage pour les réplicas d'objets, comme suit :

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
       <StorageClass>storage-class</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Vous pouvez spécifier n'importe quelle classe de stockage prise en charge par Amazon S3.

Example 2 : Configuration de réplication à deux règles

Example

Dans la configuration de réplication suivante, les règles spécifient les éléments suivants :

- Chaque règle filtre un préfixe de clé différent afin que chaque règle s'applique à un sous-ensemble distinct d'objets. Dans cet exemple, Simple Storage Service (Amazon S3) réplique les objets avec les noms de clé *Tax/doc1.pdf* et *Project/project1.txt*, mais ne réplique pas les objets avec le nom de clé *PersonalDoc/documentA*.
- Bien que les deux règles spécifient une valeur pour l'élément <Priority>, la priorité des règles n'a aucune importance car les règles s'appliquent à deux ensembles d'objets distincts. L'exemple suivant décrit ce qui se passe lorsque la priorité des règles est appliquée.
- La deuxième règle spécifie la classe de stockage S3 Standard-Accès peu fréquent pour les réplicas d'objets. Simple Storage Service (Amazon S3) utilise la classe de stockage spécifiée pour ces réplicas d'objets.

```
<?xml version="1.0" encoding="UTF-8"?>

<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
     ...
  </Rule>
 <Rule>
    <Status>Enabled</Status>
```

```
    <Priority>2</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>Project</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
     <StorageClass>STANDARD_IA</StorageClass>
    </Destination>
     ...
  </Rule>


</ReplicationConfiguration>
```

Example 3 : Configuration de réplication à deux règles et avec des préfixes qui se chevauchent

Dans cette configuration, les deux règles indiquent des filtres avec des préfixes de clé se chevauchant, *star/* et *starship/*. Les deux règles s'appliquent aux objets portant le nom de clé *starship-x*. Dans ce cas, Amazon S3 utilise la priorité des règles pour déterminer la règle à appliquer. Plus le nombre est élevé, plus la priorité est haute.

```
<ReplicationConfiguration>

  <Role>arn:aws:iam::account-id:role/role-name</Role>

  <Rule>
    <Status>Enabled</Status>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>star</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
  <Rule>
```

```
    <Status>Enabled</Status>
    <Priority>2</Priority>
    <DeleteMarkerReplication>
       <Status>string</Status>
    </DeleteMarkerReplication>
    <Filter>
        <Prefix>starship</Prefix>
    </Filter>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Example 4 : Exemples de procédures

Pour afficher des exemples, consultez Exemples de configuration de la réplication en direct.

Pour plus d'informations sur la structure XML de la configuration de réplication, consultez PutBucketReplicationle manuel Amazon Simple Storage Service API Reference.

Considérations relatives à la rétrocompatibilité

La dernière version du format XML de configuration de réplication est V2. Les configurations de réplication XML V2 sont celles qui contiennent l'élément `<Filter>` pour les règles et les règles qui spécifient le contrôle du délai de réplication S3.

Pour afficher votre version de configuration de réplication, vous pouvez utiliser l'opération d'API `GetBucketReplication`. Pour plus d'informations, consultez GetBucketReplication dans la Référence d'API Amazon Simple Storage Service.

Pour assurer la rétrocompatibilité, Amazon S3 continue de prendre en charge le format de configuration de réplication XML V1. Si vous avez utilisé la configuration de réplication XML V1, tenez compte des problèmes suivants qui ont un impact sur la rétrocompatibilité :

- Le format de configuration de réplication XML V2 inclut l'élément `<Filter>` pour les règles. L'élément `<Filter>` vous permet de spécifier des filtres d'objet basés sur le préfixe de clé d'objet et/ou des balises pour définir la portée des objets auxquels la règle s'applique. Le format de configuration de réplication XML V1 prend en charge un filtrage basé uniquement sur le préfixe de la clé. Dans ce cas, vous ajoutez directement l'élément `<Prefix>` en tant qu'élément enfant de l'élément `<Rule>`, comme dans l'exemple suivant :

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Role>arn:aws:iam::account-id:role/role-name</Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
       <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
    </Destination>

  </Rule>
</ReplicationConfiguration>
```

- Lorsque vous supprimez un objet de votre compartiment source, sans spécifier d'ID de version d'objet, Simple Storage Service (Amazon S3) ajoute un marqueur de suppression. Si vous utilisez le format de configuration de réplication XML V1, Amazon S3 réplique uniquement les marqueurs de suppression créés par les actions utilisateur. En d'autres termes, Amazon S3 réplique le marqueur de suppression uniquement si un utilisateur supprime un objet. Si un objet ayant expiré est supprimé par Amazon S3 (dans le cadre d'une action de cycle de vie), Amazon S3 ne réplique pas le marqueur de suppression.

  Dans le format XML V2 de configuration de réplication, vous pouvez activer la réplication des marqueurs de suppression pour non-tag-based les règles. Pour de plus amples informations, veuillez consulter Répliquer des marqueurs de suppression entre les compartiments.

Configuration des autorisations pour la réplication en direct

Lors de la configuration de la réplication en direct dans Amazon S3, vous devez acquérir les autorisations nécessaires, comme suit :

- Simple Storage Service (Amazon S3) a besoin d'autorisations pour répliquer des objets en votre nom. Vous accordez ces autorisations en créant un rôle AWS Identity and Access Management (IAM), puis en spécifiant ce rôle dans votre configuration de réplication.
- Lorsque les compartiments source et de destination n'appartiennent pas aux mêmes comptes, le propriétaire du compartiment de destination doit accorder au propriétaire du compartiment source les autorisations adéquates pour stocker les réplicas.

Rubriques

- Configuration des autorisations pour créer des règles de réplication
- Création d'un rôle IAM
- Octroi d'autorisations lorsque les compartiments source et de destination appartiennent à des entités différentes Comptes AWS
- Modification du propriétaire d'un réplica
- Octroi d'autorisations pour les opérations par lots S3

Configuration des autorisations pour créer des règles de réplication

L'utilisateur ou le rôle IAM que vous allez utiliser pour créer des règles de réplication a besoin d'autorisations pour créer des règles de réplication pour les réplications unidirectionnelles ou bidirectionnelles. Si l'utilisateur ou le rôle ne dispose pas de ces autorisations, vous ne pourrez pas créer de règles de réplication. Pour plus d'informations, consultez la section Identités IAM dans le guide de l'utilisateur IAM.

L'utilisateur ou le rôle a besoin des actions suivantes :

- `iam:AttachRolePolicy`
- `iam:CreatePolicy`
- `iam:CreateServiceLinkedRole`
- `iam:PassRole`
- `iam:PutRolePolicy`
- `s3:GetBucketVersioning`
- `s3:GetObjectVersionAcl`
- `s3:GetObjectVersionForReplication`
- `s3:GetReplicationConfiguration`
- `s3:PutReplicationConfiguration`

Voici un exemple de politique IAM qui inclut ces actions.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetAccessPoint",
                "s3:GetAccountPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:ListAccessPoints",
                "s3:ListAllMyBuckets",
                "s3:PutReplicationConfiguration",
                "s3:GetReplicationConfiguration",
                "s3:GetBucketVersioning",
                "s3:GetObjectVersionForReplication",
                "s3:GetObjectVersionAcl",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetObjectVersion",
                "s3:GetBucketOwnershipControls",
                "s3:PutBucketOwnershipControls",
                "s3:GetObjectLegalHold",
                "s3:GetObjectRetention",
                "s3:GetBucketObjectLockConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-bucket1-*",
                "arn:aws:s3:::amzn-s3-demo-bucket2-*/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:List*AccessPoint*",
                "s3:GetMultiRegion*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
```

```
                "iam:Get*",
                "iam:CreateServiceLinkedRole",
                "iam:CreateRole",
                "iam:PassRole"
            ],
            "Resource": "arn:aws:iam::*:role/service-role/s3*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:AttachRolePolicy",
                "iam:PutRolePolicy",
                "iam:CreatePolicy"
              ],
            "Resource": [
                "arn:aws:iam::*:policy/service-role/s3*",
                "arn:aws:iam::*:role/service-role/s3*"
            ]
        }
    ]
}
```

Création d'un rôle IAM

Par défaut, toutes les ressources Simple Storage Service (Amazon S3) (compartiments, objets et sous-ressources liées) sont privées : seul le propriétaire des ressources peut y accéder. Simple Storage Service (Amazon S3) a besoin d'autorisations pour lire et répliquer les objets du compartiment source. Vous accordez ces autorisations en créant un rôle IAM et en spécifiant ce rôle dans votre configuration de réplication.

Cette section décrit la politique d'approbation et la politique d'autorisations minimales requises qui sont attachées à ce rôle IAM. Les exemples de procédures pas à pas fournissent des step-by-step

instructions pour créer un rôle IAM. Pour de plus amples informations, veuillez consulter Exemples de configuration de la réplication en direct.

La politique d'approbation identifie les identités de principal qui peuvent endosser le rôle IAM. La politique d'autorisations spécifie les actions que peut exécuter le rôle IAM, sur quelles ressources et dans quelles conditions.

- L'exemple suivant montre une politique de confiance dans laquelle vous identifiez Amazon S3 comme le Service AWS principal habilité à assumer le rôle :

  JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

- L'exemple suivant illustre une politique d'approbation permettant d'identifier Amazon S3 et les opérations par lot S3 en tant que principaux de service capables d'endosser le rôle. utilisez cette approche si vous créez une tâche de réplication par lot. Pour de plus amples informations, veuillez consulter Créer une tâche de réplication par lot pour de nouvelles destinations ou règles de réplication.

  JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service": [
              "s3.amazonaws.com",
              "batchoperations.s3.amazonaws.com"
```

```
            ]
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

Pour plus d'informations sur les rôles IAM, consultez Rôles IAM dans le manuel IAM Guide de l'utilisateur.

- L'exemple suivant illustre une politique d'autorisations permettant d'accorder au rôle IAM les autorisations d'effectuer les tâches de réplication en votre nom. Quand Simple Storage Service (Amazon S3) endosse le rôle, il dispose des autorisations que vous avez spécifiées dans cette stratégie. Dans cette politique, *amzn-s3-demo-source-bucket* est le compartiment source et *amzn-s3-demo-destination-bucket*, le compartiment de destination.

  JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
```

```
            "Effect":"Allow",
            "Action":[
               "s3:ReplicateObject",
               "s3:ReplicateDelete",
               "s3:ReplicateTags"
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
         }
      ]
}
```

La politique d'autorisations accorde des autorisations pour les actions suivantes :

- `s3:GetReplicationConfiguration` et `s3:ListBucket` : les autorisations d'exécuter ces actions sur le compartiment *amzn-s3-demo-source-bucket* permettent à Amazon S3 de récupérer la configuration de réplication et de répertorier le contenu du compartiment. (Le modèle d'autorisations actuel nécessite l'autorisation `s3:ListBucket` pour accéder aux marqueurs de suppression.)
- `s3:GetObjectVersionForReplication` et `s3:GetObjectVersionAcl` – Les autorisations d'effectuer ces actions accordées sur tous les objets permettent à Simple Storage Service (Amazon S3) d'obtenir une version d'objet particulière et la liste de contrôle d'accès (ACL) associée aux objets.

- `s3:ReplicateObject` et `s3:ReplicateDelete` – Les autorisations d'effectuer ces actions sur des objets du compartiment *amzn-s3-demo-destination-bucket* permettent à Simple Storage Service (Amazon S3) de répliquer des objets ou des marqueurs de suppression dans le compartiment de destination. Pour de plus amples informations sur les marqueurs de suppression, consultez Impact des opérations de suppression sur la réplication.

  > **Note**
  >
  > Les autorisations relatives à l'`s3:ReplicateObject`action sur le *amzn-s3-demo-destination-bucket* compartiment autorisent également la réplication de métadonnées telles que les balises d'objet et ACLs. Il n'est donc pas nécessaire d'accorder une autorisation explicite pour l'action `s3:ReplicateTags`.

- `s3:GetObjectVersionTagging` : les autorisations d'exécuter cette action sur des objets du compartiment *amzn-s3-demo-source-bucket* permettent à Amazon S3 de lire les balises d'objets pour la réplication. Pour en savoir plus sur les balises d'objet, consultez

Catégorisation de vos objets à l'aide de balises. Si Amazon S3 ne dispose pas de l'autorisation `s3:GetObjectVersionTagging`, il réplique les objets mais pas leurs balises.

Pour afficher la liste des actions Amazon S3, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Important

Le Compte AWS titulaire du rôle IAM doit disposer des autorisations pour les actions qu'il accorde au rôle IAM.
Supposons, par exemple, que le compartiment source contient des objets détenus par un autre Compte AWS. Le propriétaire des objets doit explicitement accorder à Compte AWS celui qui détient le rôle IAM les autorisations requises par le biais des listes de contrôle d'accès des objets ()ACLs. Dans le cas contraire, Amazon S3 ne peut pas accéder aux objets et la réplication des objets échoue. Pour plus d'informations sur les autorisations ACL, consultez Présentation de la liste de contrôle d'accès (ACL).
Les autorisations décrites dans la présente section sont liées à la configuration de réplication minimale. Si vous choisissez d'ajouter des configurations de réplication facultatives, vous devez accorder des autorisations supplémentaires à Amazon S3 :

- Pour répliquer des objets chiffrés, vous devez également accorder les autorisations clés AWS Key Management Service (AWS KMS) nécessaires. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets chiffrés".
- Pour utiliser Object Lock avec la réplication, vous devez accorder deux autorisations supplémentaires sur le compartiment S3 source dans le rôle AWS Identity and Access Management (IAM) que vous utilisez pour configurer la réplication.
  Les deux autorisations supplémentaires sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d'une déclaration d'autorisation `s3:Get*`, cette déclaration répond à l'exigence. Pour de plus amples informations, veuillez consulter the section called "Utilisation du verrouillage d'objet avec la réplication S3".

Octroi d'autorisations lorsque les compartiments source et de destination appartiennent à des entités différentes Comptes AWS

Lorsque les compartiments source et de destination n'appartiennent pas aux mêmes comptes, le propriétaire du compartiment de destination doit également ajouter une politique de compartiment pour accorder au propriétaire du compartiment source les autorisations adéquates pour effectuer des actions de réplication, comme illustré dans l'exemple suivant. Dans cette exemple de politique, *amzn-s3-demo-destination-bucket* est le compartiment de destination.

Vous pouvez également laisser la console Amazon S3 générer automatiquement cette politique de compartiment à votre place. Pour plus d'informations, consultez Activer la réception d'objets répliqués à partir d'un compartiment source.

> **Note**
>
> Le format ARN du rôle peut être différent. Si le rôle a été créé à l'aide de la console, le format ARN est `arn:aws:iam::`*account-ID*`:role/service-role/`*role-name*. Si le rôle a été créé à l'aide du AWS CLI, le format ARN est`arn:aws:iam::`*account-ID*`:role/`*role-name*. Pour plus d'informations, consultez Rôles IAM dans le Guide de l'utilisateur IAM.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "PolicyForDestinationBucket",
    "Statement": [
        {
            "Sid": "Permissions on objects",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/source-
account-IAM-role"
            },
            "Action": [
                "s3:ReplicateDelete",
                "s3:ReplicateObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
```

```
        },
        {
            "Sid": "Permissions on bucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/source-
account-IAM-role"
            },
            "Action": [
                "s3:List*",
                "s3:GetBucketVersioning",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3::amzn-s3-demo-destination-bucket"
        }
    ]
}
```

Pour obtenir un exemple, consultez Configuration de la réplication pour des compartiments dans des comptes distincts.

Si des objets stockés dans le compartiment source sont balisés, notez les points suivants :

- Si le propriétaire du compartiment source octroie à Amazon S3 l'autorisation d'effectuer les actions `s3:GetObjectVersionTagging` et `s3:ReplicateTags` en vue de répliquer des balises d'objets (via le rôle IAM), Amazon S3 réplique les balises en même temps que les objets. Pour obtenir des informations sur le rôle IAM, consultez Création d'un rôle IAM.
- Si le propriétaire du compartiment de destination ne souhaite pas répliquer les balises, il peut ajouter l'instruction suivante à la stratégie du compartiment de destination en vue de lui refuser explicitement l'autorisation d'exécuter l'action `s3:ReplicateTags`. Dans cette politique, *amzn-s3-demo-destination-bucket* est le compartiment de destination.

```
...
   "Statement":[
      {
         "Effect":"Deny",
         "Principal":{
            "AWS":"arn:aws:iam::source-bucket-account-id:role/service-role/source-
account-IAM-role"
         },
         "Action":"s3:ReplicateTags",
```

```
        "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
...
```

> **Note**
>
> - Si vous souhaitez répliquer des objets chiffrés, vous devez également accorder les autorisations clés AWS Key Management Service (AWS KMS) nécessaires. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets chiffrés".
> - Pour utiliser Object Lock avec la réplication, vous devez accorder deux autorisations supplémentaires sur le compartiment S3 source dans le rôle AWS Identity and Access Management (IAM) que vous utilisez pour configurer la réplication. Les deux autorisations supplémentaires sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d'une déclaration d'autorisation `s3:Get*`, cette déclaration répond à l'exigence. Pour de plus amples informations, veuillez consulter the section called "Utilisation du verrouillage d'objet avec la réplication S3".

Activation de la réception d'objets répliqués à partir d'un compartiment source

Au lieu d'ajouter manuellement la politique précédente à votre compartiment de destination, vous pouvez rapidement générer les politiques nécessaires pour activer la réception d'objets répliqués à partir d'un compartiment source via la console Amazon S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le compartiment que vous souhaitez utiliser comme compartiment de destination.
4. Choisissez l'onglet Management (Gestion), puis faites défiler jusqu'à Replication rules (Règles de réplication).
5. Pour Actions, choisissez Receive replicated objects (Recevoir des objets répliqués).

Suivez les instructions et entrez l' Compte AWS ID du compte du compartiment source, puis choisissez Generate policies. La console génère une politique de compartiment Amazon S3 et une stratégie de clé KMS.

6. Pour ajouter cette politique à votre politique de compartiment existante, choisissez Apply settings (Appliquer les paramètres) ou Copy (Copier) pour copier manuellement les modifications.
7. (Facultatif) Copiez la AWS KMS politique dans la politique de clé KMS de votre choix dans la AWS Key Management Service console.

Modification du propriétaire d'un réplica

Si différents Comptes AWS propriétaires des compartiments source et de destination sont propriétaires, vous pouvez demander à Amazon S3 de remplacer le propriétaire de la réplique par Compte AWS celui qui détient le compartiment de destination. Pour plus d'informations sur l'option de substitution du propriétaire, consultez Modification du propriétaire d'un réplica.

Octroi d'autorisations pour les opérations par lots S3

La réplication par lot S3 vous permet de répliquer les objets suivants :

- Objets qui existaient avant la mise en place d'une configuration de réplication
- Objets qui ont déjà été répliqués
- Objets dont la réplication a échoué

Vous pouvez créer une tâche de réplication par lot unique lors de la création de la première règle dans une nouvelle configuration de réplication ou de l'ajout d'une nouvelle destination à une configuration existante via la console Amazon S3. Vous pouvez également lancer la réplication par lot pour une configuration de réplication existante en créant une tâche d'opérations par lot.

Pour des exemples de politiques et de rôles IAM de réplication par lot, consultez Configuration d'un rôle IAM pour la réplication par lot S3.

Exemples de configuration de la réplication en direct

Les exemples suivants fournissent des step-by-step procédures pas à pas qui montrent comment configurer la réplication en direct pour les cas d'utilisation courants.

> **Note**
>
> La réplication en direct fait référence à la réplication dans une même région (SRR) et une réplication entre régions (CRR). La réplication en direct ne réplique pas les objets qui existaient dans le compartiment avant la configuration de la réplication. Pour répliquer des objets qui existaient avant la configuration de la réplication, utilisez la réplication à la demande. Pour synchroniser des compartiments et répliquer des objets existants à la demande, consultez Réplication d'objets existants.

Ces exemples montrent comment créer une configuration de réplication à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI)AWS SDK pour Java et AWS SDKs (AWS SDK pour .NET des exemples sont présentés).

Pour plus d'informations sur l'installation et la configuration du AWS CLI, consultez les rubriques suivantes du Guide de AWS Command Line Interface l'utilisateur :

- Commencez avec le AWS CLI
- Configurer le AWS CLI — Vous devez configurer au moins un profil. Si vous explorez des scénarios entre comptes, configurez deux profils.

Pour plus d'informations sur le AWS SDKs, reportez-vous AWS SDK pour Javaaux sections et AWS SDK pour .NET.

> **Tip**
>
> Pour un step-by-step didacticiel expliquant comment utiliser la réplication en direct pour répliquer des données, voir Tutoriel : Réplication de données dans et entre les deux à Régions AWS l'aide de S3 Replication.

Rubriques

- Configuration d'une réplication pour des compartiments dans le même compte
- Configuration de la réplication pour des compartiments dans des comptes distincts
- Satisfaction aux exigences de conformité à l'aide du contrôle du temps de réplication S3
- Réplication d'objets chiffrés (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C)

- Réplication des modifications des métadonnées avec la synchronisation des modifications de réplica
- Répliquer des marqueurs de suppression entre les compartiments

Configuration d'une réplication pour des compartiments dans le même compte

La réplication dynamique est la copie automatique et asynchrone d'objets dans des compartiments à usage général, identiques ou différents. Régions AWS La réplication en direct copie les objets nouvellement créés et les mises à jour d'objets à partir d'un compartiment source vers un ou plusieurs compartiments de destination. Pour de plus amples informations, veuillez consulter Réplication d'objets au sein des régions et entre elles.

Lorsque vous configurez la réplication, vous ajoutez des règles de réplication au compartiment source. Les règles de réplication définissent les objets du compartiment source à répliquer, ainsi que le ou les compartiments de destination dans lesquels les objets répliqués seront stockés. Vous pouvez créer une règle pour répliquer tous les objets ou un sous-ensemble d'objets d'un compartiment à l'aide de préfixes de nom de clé ou d'autres balises d'objet, ou les deux. Un compartiment de destination peut se trouver dans le même compartiment Compte AWS que le compartiment source ou dans un autre compte.

Si vous spécifiez un ID de version d'objet à supprimer, Amazon S3 supprime cette version de l'objet dans le compartiment source. Mais le service ne réplique pas la suppression dans le compartiment de destination. En d'autres termes, il ne supprime pas la même version de l'objet dans le compartiment de destination. Les données sont ainsi protégées contre les suppressions malveillantes.

Lorsque vous ajoutez une règle de réplication à un compartiment, celle-ci est activée par défaut et entre en fonctionnement dès que vous l'enregistrez.

Dans cet exemple, vous configurez la réplication en direct pour les compartiments source et de destination qui appartiennent au même Compte AWS. Des exemples d'utilisation de la console Amazon S3, du AWS Command Line Interface (AWS CLI) et du AWS SDK pour Java and sont fournis AWS SDK pour .NET.

Prérequis

Avant d'utiliser les procédures suivantes, assurez-vous d'avoir configuré les autorisations nécessaires pour la réplication, selon que les compartiments source et de destination appartiennent au même

compte ou à des comptes différents. Pour de plus amples informations, veuillez consulter the section called "Configurer les autorisations".

> **Note**
>
> - Si vous souhaitez répliquer des objets chiffrés, vous devez également accorder les autorisations clés AWS Key Management Service (AWS KMS) nécessaires. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets chiffrés".
> - Pour utiliser Object Lock avec la réplication, vous devez accorder deux autorisations supplémentaires sur le compartiment S3 source dans le rôle AWS Identity and Access Management (IAM) que vous utilisez pour configurer la réplication. Les deux autorisations supplémentaires sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d'une déclaration d'autorisation `s3:Get*`, cette déclaration répond à l'exigence. Pour de plus amples informations, veuillez consulter the section called "Utilisation du verrouillage d'objet avec la réplication S3".

Utilisation de la console S3

Pour configurer une règle de réplication lorsque le compartiment de destination se trouve dans le même compartiment Compte AWS que le compartiment source, procédez comme suit.

Si le compartiment de destination se trouve dans un compte différent du compartiment source, vous devez ajouter une politique de compartiment au compartiment de destination pour accorder au propriétaire du compte du compartiment source l'autorisation d'effectuer des réplications d'objets dans le compartiment de destination. Pour de plus amples informations, veuillez consulter Octroi d'autorisations lorsque les compartiments source et de destination appartiennent à des entités différentes Comptes AWS.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment que vous souhaitez.
4. Sélectionnez Gestion, faites défiler jusqu'à Règles de réplication, puis sélectionnez Créer une règle de réplication.

5. Dans la section Configuration de la règle de réplication, sous Nom de la règle de réplication, saisissez un nom pour votre règle afin de l'identifier facilement plus tard. Ce nom est obligatoire et doit être unique dans le compartiment.
6. Sous Statut, Activé est sélectionné par défaut. Un règle activée entre en fonctionnement dès que l'avez enregistrée. Si vous souhaitez activer la règle ultérieurement, sélectionnez Désactivé.
7. Si le compartiment possède des règles de réplication existantes, il vous est demandé de définir une priorité pour la règle. Vous devez définir une priorité pour la règle pour éviter les conflits provoqués par les objets inclus dans l'étendue de plusieurs règles. En cas de chevauchement de règles, Amazon S3 utilise la priorité des règles pour déterminer la règle à appliquer. Plus le nombre est élevé, plus la priorité est haute. Pour plus d'informations sur la priorité des règles, consultez Éléments du fichier de configuration de réplication.
8. Sous Compartiment source, vous disposez des options suivantes pour définir la source de réplication :

   - Pour répliquer l'ensemble du compartiment, choisissez Apply to all objects in the bucket (Appliquer à tous les objets du compartiment).
   - Pour répliquer tous les objets ayant le même préfixe, choisissez Limit the scope of this rule using one or more filters (Limiter la portée de cette règle en utilisant un ou plusieurs filtres). Cela limite la réplication à tous les objets dont les noms commencent par le préfixe que vous spécifiez (par exemple, `pictures`). Saisissez un préfixe dans la zone Préfixe.

     > **Note**
     >
     > Si vous entrez un préfixe correspondant à un nom de dossier, vous devez insérer le caractère / (barre oblique) à la fin (par exemple, `pictures/`).

   - Pour répliquer tous les objets avec une ou plusieurs balises d'objet, sélectionnez Ajouter une balise et saisissez la paire clé-valeur dans les zones. Répétez la procédure pour ajouter une autre balise. Vous pouvez combiner un préfixe et des balises. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.

   Le nouveau schéma XML de configuration de la réplication prend en charge le balisage de préfixe et de balise, et la priorité des règles. Pour plus d'informations sur le nouveau schéma, consultez Considérations relatives à la rétrocompatibilité. Pour plus d'informations sur le XML utilisé avec l'API Amazon S3 qui fonctionne derrière l'interface utilisateur, reportez-vous à

Éléments du fichier de configuration de réplication. Le nouveau schéma est décrit comme configuration de réplication XML V2.

9. Sous Destination, sélectionnez le compartiment où vous souhaitez qu'Amazon S3 réplique les objets.

> **Note**
>
> Le nombre de compartiments de destination est limité au nombre de compartiments contenus Régions AWS dans une partition donnée. Une partition est un regroupement de régions. AWS possède actuellement trois partitions : `aws` (Régions standard), `aws-cn` (Régions de Chine) et `aws-us-gov` (AWS GovCloud (US) Régions). Vous pouvez utiliser Service Quotas pour demander une augmentation de votre limite de compartiments de destination.

- Pour répliquer vers un compartiment ou plusieurs compartiments de votre compte, sélectionnez Choisir un compartiment dans ce compte et saisissez ou recherchez le nom du compartiment de destination.
- Pour effectuer une réplication vers un ou plusieurs compartiments d'un autre compte Compte AWS, choisissez Spécifier un compartiment dans un autre compte, puis entrez l'ID du compte du compartiment de destination et le nom du compartiment.

  Si la destination se trouve dans un compte différent du compartiment source, vous devez ajouter une politique de compartiment aux compartiments de destination pour accorder au propriétaire du compte du compartiment source l'autorisation d'effectuer des réplications d'objets. Pour plus d'informations, consultez Octroi d'autorisations lorsque les compartiments source et de destination appartiennent à des entités différentes Comptes AWS.

  (Facultatif) Si vous souhaitez aider à normaliser la propriété des nouveaux objets dans le compartiment de destination, choisissez Remplacer la propriété de l'objet par le propriétaire du compartiment de destination. Pour plus d'informations sur cette option, consultez Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

> **Note**
>
> Si la gestion des versions n'est pas activée sur le compartiment de destination, un message d'avertissement avec le bouton Activer la gestion des versions s'affiche. Cliquez sur ce bouton pour activer la gestion des versions sur le compartiment.

10. Configurez un rôle AWS Identity and Access Management (IAM) qu'Amazon S3 peut assumer pour répliquer des objets en votre nom.

    Pour configurer un rôle IAM, dans la section Rôle IAM, sélectionnez l'une des options suivantes dans la liste déroulante des rôles IAM :

    - Nous vous recommandons vivement de choisir Create new role (Créer un nouveau rôle) pour demander à Amazon S3 de créer nouveau rôle IAM pour vous. Lorsque vous enregistrez la règle, une nouvelle stratégie est générée pour le rôle IAM correspondant aux compartiments source et cible que vous choisissez.
    - Vous pouvez également choisir d'utiliser un rôle IAM existant. Dans ce cas, vous devez choisir un rôle qui octroie à Amazon S3 les autorisations nécessaires pour la réplication. La réplication échoue si ce rôle n'accorde pas à Amazon S3 les autorisations suffisantes pour suivre votre règle de réplication.

    > **Important**
    >
    > Lorsque vous ajoutez une règle de réplication à un compartiment, vous devez disposer de l'autorisation `iam:PassRole` pour pouvoir transmettre le rôle IAM qui accorde les autorisations de réplication Amazon S3. Pour plus d'informations, consultez Octroi d'autorisations à un utilisateur pour transférer un rôle à un Service AWS dans le Guide de l'utilisateur IAM.

11. Pour répliquer les objets du compartiment source chiffrés à l'aide du chiffrement côté serveur à l'aide de clés AWS Key Management Service (AWS KMS) (SSE-KMS), sous Chiffrement, sélectionnez Répliquer les objets chiffrés avec. AWS KMS Sous Clés AWS KMS pour le chiffrement des objets de destination se trouvent les clés source que la réplication est autorisée à utiliser. Toutes les clés source KMS sont incluses par défaut. Vous pouvez choisir un alias ou un ID de clé afin de restreindre la sélection des clés KMS.

Les objets chiffrés par AWS KMS keys ceux que vous ne sélectionnez pas ne sont pas répliqués. Une clé KMS ou un groupe de clés KMS est sélectionné pour vous, mais vous pouvez choisir les clés KMS que vous souhaitez utiliser si vous le souhaitez. Pour plus d'informations sur l'utilisation AWS KMS avec la réplication, consultezRéplication d'objets chiffrés (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).

> **Important**
>
> Lorsque vous répliquez des objets chiffrés avec AWS KMS, le taux de AWS KMS demandes double dans la région source et augmente d'autant dans la région de destination. Ces taux d'appels accrus AWS KMS sont dus à la manière dont les données sont rechiffrées à l'aide de la clé KMS que vous définissez pour la région de destination de la réplication. AWS KMS dispose d'un quota de taux de demandes par compte d'appel et par région. Pour obtenir des informations sur les quotas par défaut, consultez Quotas AWS KMS – nombre de demandes par seconde : variable dans le Guide du développeur AWS Key Management Service .
>
> Si votre taux actuel de demandes d'PUTobjets Amazon S3 pendant la réplication est supérieur à la moitié de la limite de AWS KMS débit par défaut de votre compte, nous vous recommandons de demander une augmentation de votre quota de taux de AWS KMS demandes. Pour demander une augmentation, contactez-nous afin de créer un cas dans le Centre Support . Supposons, par exemple, que votre taux de demandes d'PUTobjets actuel soit de 1 000 requêtes par seconde et que vous l'utilisiez AWS KMS pour chiffrer vos objets. Dans ce cas, nous vous recommandons de demander Support à augmenter votre limite de AWS KMS débit à 2 500 requêtes par seconde, à la fois dans vos régions source et de destination (si elles sont différentes), afin de garantir qu'il n'y ait pas de limitation. AWS KMS
>
> Pour connaître le taux de demandes d'PUTobjets dans le compartiment source, consultez `PutRequests` les métriques des CloudWatch demandes Amazon pour Amazon S3. Pour plus d'informations sur l'affichage CloudWatch des métriques, consultezUtiliser la console S3..

Si vous avez choisi de répliquer des objets chiffrés avec AWS KMS, procédez comme suit :

- Sous AWS KMS key pour le chiffrement des objets de destination, spécifiez votre clé KMS de l'une des manières suivantes :

- Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos clés AWS KMS keys, puis sélectionnez votre Clé KMS dans la liste des clés disponibles.

  La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

- Pour saisir l'Amazon Resource Name (ARN) de la clé KMS, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de votre clé KMS dans le champ qui s'affiche. Cela chiffre les réplicas dans le compartiment de destination. Vous trouverez l'ARN de votre clé KMS dans la console IAM, sous Clés de chiffrement.
- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

  Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur.

> **Important**
>
> Vous ne pouvez utiliser que les clés KMS activées au même endroit Région AWS que le bucket. Lorsque vous choisissez Choisir parmi vos clés KMS, la console S3 ne répertorie que 100 clés KMS par région. Si vous avez plus de 100 clés KMS dans la même Région, vous pourrez uniquement afficher les 100 premières clés KMS dans la console S3. Pour utiliser une clé KMS qui n'est pas répertoriée dans la console, choisissez Saisir l'ARN de AWS KMS key , puis saisissez l'ARN de la clé KMS.
> Lorsque vous utilisez un AWS KMS key pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé KMS de chiffrement symétrique. Amazon S3 prend uniquement en charge les clés KMS symétriques de chiffrement et ne prend pas en charge les clés KMS asymétriques. Pour plus d'informations, consultez Identification des clés KMS symétriques et asymétriques dans le Guide du développeur AWS Key Management Service .

Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le Guide du AWS Key Management Service développeur. Pour plus d'informations

sur l'utilisation AWS KMS avec Amazon S3, consultezUtilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

12. Sous Classe de stockage de destination, si vous voulez répliquer vos données dans une classe de stockage spécifique dans le compartiment de destination, sélectionnez Modifier la classe de stockage pour les objets répliqués. Choisissez ensuite la classe de stockage que vous voulez utiliser pour les objets répliqués dans la destination. Si vous ne sélectionnez pas cette option, la classe de stockage utilisée pour les objets répliqués est identique à celle des objets d'origine.
13. Vous disposez des options supplémentaires suivantes lors de la définition des Options de réplication supplémentaires :

    - Si vous souhaitez activer le Contrôle du temps de réplication S3 (S3 RTC) dans votre configuration de réplication, sélectionnez Contrôle du délai de réplication (RTC). Pour plus d'informations sur cette option, consultez Satisfaction aux exigences de conformité à l'aide du contrôle du temps de réplication S3.
    - Si vous souhaitez activer les métriques de réplication S3 dans votre configuration de réplication, sélectionnez Replication metrics and events (Métriques et événements de réplication). Pour de plus amples informations, veuillez consulter Surveillance de la réplication avec des métriques, des notifications d'événements et des statuts.
    - Si vous souhaitez activer la réplication de marqueurs de suppression dans votre configuration de réplication, sélectionnez Réplication des marqueurs de suppression. Pour de plus amples informations, veuillez consulter Répliquer des marqueurs de suppression entre les compartiments.
    - Si vous souhaitez activer la synchronisation des modifications de réplica Amazon S3 dans votre configuration de réplication, sélectionnez Synchronisation des modifications de réplica. Pour de plus amples informations, veuillez consulter Réplication des modifications des métadonnées avec la synchronisation des modifications de réplica.

    > **Note**
    >
    > Des frais supplémentaires s'appliquent lorsque vous utilisez des métriques de réplication S3 RTC ou S3.

14. Pour terminer, choisissez Enregistrer.
15. Une fois votre règle enregistrée, vous pouvez la modifier, l'activer, la désactiver ou la supprimer en la sélectionnant et en choisissant Edit rule (Modifier la règle).

À l'aide du AWS CLI

AWS CLI Pour configurer la réplication lorsque les compartiments source et de destination appartiennent à la même entité Compte AWS, procédez comme suit :

- Créez des compartiments source et de destination.
- Activez la gestion des versions sur ces compartiments.
- Créez un rôle AWS Identity and Access Management (IAM) qui autorise Amazon S3 à répliquer des objets.
- Ajoutez la configuration de réplication au compartiment source.

Testez votre configuration pour la vérifier.

Pour configurer la réplication lorsque les compartiments source et de destination appartiennent à la même entité Compte AWS

1. Définissez un profil d'informations d'identification pour l' AWS CLI. Cet exemple utilise le nom de profil `acctA`. Pour obtenir des informations sur la définition des profils d'informations d'identification et l'utilisation de profils nommés, consultez Paramètres des fichiers de configuration et d'informations d'identification dans le Guide de l'utilisateur AWS Command Line Interface .

   > **Important**
   >
   > Le profil que vous utilisez dans cet exemple doit disposer des autorisations nécessaires. Par exemple, dans la configuration de réplication, vous spécifiez le rôle IAM qu'Amazon S3 peut endosser. Vous ne pouvez effectuer cette tâche que si le profil que vous utilisez dispose de l'autorisation `iam:PassRole`. Pour plus d'informations, consultez Octroi d'autorisations à un utilisateur pour transférer un rôle à un Service AWS dans le Guide de l'utilisateur IAM. Si vous utilisez les informations d'identification d'un administrateur pour créer un profil nommé, vous pouvez exécuter toutes les tâches.

2. Créez un compartiment source et activez la gestion des versions sur celui-ci en utilisant les commandes AWS CLI suivantes. Pour utiliser ces commandes, remplacez *`user input placeholders`* par vos propres informations.

   La commande `create-bucket` suivante crée un compartiment source nommé *`amzn-s3-demo-source-bucket`* dans la région USA Est (Virginie du Nord) (`us-east-1`) :

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

La commande `put-bucket-versioning` suivante active la gestion des versions S3 sur le compartiment *amzn-s3-demo-source-bucket* :

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. Créez un compartiment de destination et activez le versionnement sur celui-ci à l'aide des AWS CLI commandes suivantes. Pour utiliser ces commandes, remplacez *user input placeholders* par vos propres informations.

> **Note**
>
> Pour configurer une configuration de réplication lorsque les compartiments source et de destination se trouvent dans les mêmes compartiments Compte AWS, vous utilisez le même profil pour les compartiments source et de destination. Cet exemple utilise `acctA`. Pour tester une configuration de réplication lorsque les buckets appartiennent à différents propriétaires Comptes AWS, spécifiez des profils différents pour chaque compte. Par exemple, utilisez un profil `acctB` pour le compartiment de destination.

La commande `create-bucket` suivante crée un compartiment de destination nommé *amzn-s3-demo-destination-bucket* dans la région USA Ouest (Oregon) (`us-west-2`) :

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctA
```

La commande `put-bucket-versioning` suivante active la gestion des versions S3 sur le compartiment *amzn-s3-demo-destination-bucket* :

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

4. Créez un rôle IAM. Vous précisez ce rôle dans la configuration de réplication que vous ajouterez ultérieurement au compartiment source. Amazon S3 endosse ce rôle pour répliquer des objets en votre nom. Vous créez un rôle IAM en deux étapes.

   - Créez un rôle.
   - Attachez une stratégie d'autorisation au rôle.

   a. Créez le rôle IAM.

      i. Copiez la stratégie d'approbation suivante et enregistrez-la dans un fichier nommé `s3-role-trust-policy.json` dans le répertoire actif sur votre ordinateur local. Cette politique accorde au principal de service Amazon S3 les autorisations permettant d'endosser ce rôle.

      JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

      ii. Exécutez la commande suivante pour créer un rôle.

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

b. Attachez une stratégie d'autorisation au rôle.

i. Copiez la politique d'autorisations suivante et enregistrez-la dans un fichier nommé `s3-role-permissions-policy.json` dans le répertoire actuel de votre ordinateur local. Cette stratégie accorde des autorisations pour diverses actions sur les compartiments et les objets Amazon S3.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
```

```
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
}
```

> **Note**
>
> - Si vous souhaitez répliquer des objets chiffrés, vous devez également accorder les autorisations clés AWS Key Management Service (AWS KMS) nécessaires. Pour de plus amples informations, veuillez consulter the section called “Réplication d’objets chiffrés”.
> - Pour utiliser Object Lock avec la réplication, vous devez accorder deux autorisations supplémentaires sur le compartiment S3 source dans le rôle AWS Identity and Access Management (IAM) que vous utilisez pour configurer la réplication. Les deux autorisations supplémentaires sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d’une déclaration d’autorisation `s3:Get*`, cette déclaration répond à l’exigence. Pour de plus amples informations, veuillez consulter the section called “Utilisation du verrouillage d’objet avec la réplication S3”.

ii. Exécutez la commande suivante pour créer une stratégie et l’attacher au rôle. Remplacez *`user input placeholders`* par vos propres informations.

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-permissions-policy.json \
--policy-name replicationRolePolicy \
--profile acctA
```

5. Ajoutez une configuration de réplication au compartiment source.

   a. Bien que l'API Amazon S3 exige que vous spécifiiez la configuration de réplication au format XML, elle AWS CLI exige que vous spécifiiez la configuration de réplication au format JSON.

Enregistrez la configuration JSON dans un fichier (`replication.json`) dans le répertoire local de votre ordinateur.

```
{
  "Role": "IAM-role-ARN",
  "Rules": [
    {
      "Status": "Enabled",
      "Priority": 1,
      "DeleteMarkerReplication": { "Status": "Disabled" },
      "Filter" : { "Prefix": "Tax"},
      "Destination": {
        "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
      }
    }
  ]
}
```

b. Mettez à jour le code JSON en remplaçant les valeurs de *amzn-s3-demo-destination-bucket* et *IAM-role-ARN* par vos propres informations. Enregistrez les modifications.

c. Exécutez la commande `put-bucket-replication` suivante pour ajouter la configuration de réplication à votre compartiment source. Veillez à fournir le nom du compartiment source.

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

Pour récupérer la configuration de réplication, utilisez la commande `get-bucket-replication` :

```
$ aws s3api get-bucket-replication \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. Testez la configuration dans la console Amazon S3 en procédant comme suit :

a. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

b. Dans le panneau de navigation de gauche, choisissez Compartiments. Dans la liste Compartiments à usage général, choisissez le compartiment source.

c. Dans le compartiment source, créez un dossier nommé *Tax*.

d. Ajoutez des exemples d'objets dans le dossier *Tax* du compartiment source.

> **Note**
>
> Le temps nécessaire à Amazon S3 pour répliquer un objet dépend de la taille de l'objet. Pour obtenir des informations sur la consultation du statut de la réplication, consultez Obtention d'informations sur le statut de la réplication.

Dans le compartiment de destination, vérifiez les éléments suivants :

- Amazon S3 a répliqué les objets.
- Les objets sont des réplicas. Dans l'onglet Propriétés de vos objets, faites défiler l'affichage vers le bas jusqu'à la section Présentation de la gestion des objets. Sous Configurations de gestion, lisez la valeur sous Statut de réplication. Assurez-vous que cette valeur est définie sur `REPLICA`.
- Les réplicas appartiennent au compte du compartiment source. Vous pouvez vérifier l'appartenance des objets dans l'onglet Autorisations de vos objets.

  Si les compartiments source et de destination appartiennent à des comptes différents, vous pouvez ajouter une configuration facultative pour indiquer à Amazon S3 de remplacer le propriétaire des réplicas par le compte de destination. Pour obtenir un exemple, consultez Comment modifier le propriétaire du réplica.

À l'aide du AWS SDKs

Utilisez les exemples de code suivants pour ajouter une configuration de réplication à un compartiment avec le AWS SDK pour Java et AWS SDK pour .NET, respectivement.

> **Note**
>
> - Si vous souhaitez répliquer des objets chiffrés, vous devez également accorder les autorisations clés AWS Key Management Service (AWS KMS) nécessaires. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets chiffrés".

- Pour utiliser Object Lock avec la réplication, vous devez accorder deux autorisations supplémentaires sur le compartiment S3 source dans le rôle AWS Identity and Access Management (IAM) que vous utilisez pour configurer la réplication. Les deux autorisations supplémentaires sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d'une déclaration d'autorisation `s3:Get*`, cette déclaration répond à l'exigence. Pour de plus amples informations, veuillez consulter the section called "Utilisation du verrouillage d'objet avec la réplication S3".

Java

L'exemple suivant ajoute une configuration de réplication à un compartiment, puis la récupère et la vérifie. Pour obtenir les instructions pour la création et le test d'un exemple pratique, consultez Démarrer dans le Guide du développeur AWS SDK pour Java .

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.identitymanagement.AmazonIdentityManagement;
import
 com.amazonaws.services.identitymanagement.AmazonIdentityManagementClientBuilder;
import com.amazonaws.services.identitymanagement.model.CreateRoleRequest;
import com.amazonaws.services.identitymanagement.model.PutRolePolicyRequest;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.BucketReplicationConfiguration;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.CreateBucketRequest;
import com.amazonaws.services.s3.model.DeleteMarkerReplication;
import com.amazonaws.services.s3.model.DeleteMarkerReplicationStatus;
import com.amazonaws.services.s3.model.ReplicationDestinationConfig;
import com.amazonaws.services.s3.model.ReplicationRule;
import com.amazonaws.services.s3.model.ReplicationRuleStatus;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.replication.ReplicationFilter;
import com.amazonaws.services.s3.model.replication.ReplicationFilterPredicate;
import com.amazonaws.services.s3.model.replication.ReplicationPrefixPredicate;
```

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.HashMap;
import java.util.List;
import java.util.Map;

public class CrossRegionReplication {

        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String accountId = "*** Account ID ***";
                String roleName = "*** Role name ***";
                String sourceBucketName = "*** Source bucket name ***";
                String destBucketName = "*** Destination bucket name ***";
                String prefix = "Tax/";

                String roleARN = String.format("arn:aws:iam::%s:%s", accountId,
 roleName);
                String destinationBucketARN = "arn:aws:s3:::" + destBucketName;

                AmazonS3 s3Client = AmazonS3Client.builder()
                                .withCredentials(new ProfileCredentialsProvider())
                                .withRegion(clientRegion)
                                .build();

                createBucket(s3Client, clientRegion, sourceBucketName);
                createBucket(s3Client, clientRegion, destBucketName);
                assignRole(roleName, clientRegion, sourceBucketName,
 destBucketName);

                try {

                        // Create the replication rule.
                        List<ReplicationFilterPredicate> andOperands = new
 ArrayList<ReplicationFilterPredicate>();
                        andOperands.add(new ReplicationPrefixPredicate(prefix));

                        Map<String, ReplicationRule> replicationRules = new
 HashMap<String, ReplicationRule>();
                        replicationRules.put("ReplicationRule1",
                                        new ReplicationRule()
                                                        .withPriority(0)

 .withStatus(ReplicationRuleStatus.Enabled)
```

```
.withDeleteMarkerReplication(
                                                                    new
DeleteMarkerReplication().withStatus(

   DeleteMarkerReplicationStatus.DISABLED))
                                                        .withFilter(new
ReplicationFilter().withPredicate(
                                                                    new
ReplicationPrefixPredicate(prefix)))
                                                        .withDestinationConfig(new
ReplicationDestinationConfig()

.withBucketARN(destinationBucketARN)

.withStorageClass(StorageClass.Standard)));

                        // Save the replication rule to the source bucket.
                        s3Client.setBucketReplicationConfiguration(sourceBucketName,
                                        new BucketReplicationConfiguration()
                                                        .withRoleARN(roleARN)

.withRules(replicationRules));

                        // Retrieve the replication configuration and verify that
the configuration
                        // matches the rule we just set.
                        BucketReplicationConfiguration replicationConfig = s3Client

.getBucketReplicationConfiguration(sourceBucketName);
                        ReplicationRule rule =
replicationConfig.getRule("ReplicationRule1");
                        System.out.println("Retrieved destination bucket ARN: "
                                        +
rule.getDestinationConfig().getBucketARN());
                        System.out.println("Retrieved priority: " +
rule.getPriority());
                        System.out.println("Retrieved source-bucket replication rule
status: " + rule.getStatus());
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
couldn't process
                        // it, so it returned an error response.
                        e.printStackTrace();
```

```
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
 client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }

        private static void createBucket(AmazonS3 s3Client, Regions region, String
 bucketName) {
                CreateBucketRequest request = new CreateBucketRequest(bucketName,
 region.getName());
                s3Client.createBucket(request);
                BucketVersioningConfiguration configuration = new
 BucketVersioningConfiguration()
                                .withStatus(BucketVersioningConfiguration.ENABLED);

                SetBucketVersioningConfigurationRequest enableVersioningRequest =
 new SetBucketVersioningConfigurationRequest(
                                bucketName, configuration);
                s3Client.setBucketVersioningConfiguration(enableVersioningRequest);

        }

        private static void assignRole(String roleName, Regions region, String
 sourceBucket, String destinationBucket) {
                AmazonIdentityManagement iamClient =
 AmazonIdentityManagementClientBuilder.standard()
                                .withRegion(region)
                                .withCredentials(new ProfileCredentialsProvider())
                                .build();
                StringBuilder trustPolicy = new StringBuilder();
                trustPolicy.append("{\\r\\n   ");
                trustPolicy.append("\\\"Version\\\":\\\"2012-10-17\\\",\\r\\n   ");
                trustPolicy.append("\\\"Statement\\\":[\\r\\n      {\\r\\n
 ");
                trustPolicy.append("\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Principal\\\":{\\r\\n            ");
                trustPolicy.append("\\\"Service\\\":\\\"s3.amazonaws.com\\\"\\r\\n
      },\\r\\n         ");
                trustPolicy.append("\\\"Action\\\":\\\"sts:AssumeRole\\\"\\r\\n
  }\\r\\n   ]\\r\\n}");

                CreateRoleRequest createRoleRequest = new CreateRoleRequest()
```

```
                                .withRoleName(roleName)

 .withAssumeRolePolicyDocument(trustPolicy.toString());

                iamClient.createRole(createRoleRequest);

                StringBuilder permissionPolicy = new StringBuilder();
                permissionPolicy.append(
                                "{\\r\\n   \\\"Version\\\":\\\"2012-10-17\\\",\\r\\n
   \\\"Statement\\\":[\\r\\n      {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Action\\\":[\\r\\n             ");
                permissionPolicy.append("\\\"s3:GetObjectVersionForReplication\\\",\
\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:GetObjectVersionAcl\\\"\\r\\n         ],\\r\
\n         \\\"Resource\\\":[\\r\\n            ");
                permissionPolicy.append("\\\"arn:aws:s3:::");
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("/*\\\"\\r\\n         ]\\r\\n      },\\r\\n
     {\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Effect\\\":\\\"Allow\\\",\\r\\n         \\
\"Action\\\":[\\r\\n            ");
                permissionPolicy.append(
                                "\\\"s3:ListBucket\\\",\\r\\n            \\
\"s3:GetReplicationConfiguration\\\"\\r\\n         ");
                permissionPolicy.append("],\\r\\n         \\\"Resource\\\":[\\r\\n
          \\\"arn:aws:s3:::");
                permissionPolicy.append(sourceBucket);
                permissionPolicy.append("\\r\\n         ");
                permissionPolicy
                                .append("]\\r\\n      },\\r\\n      {\\r\\n
 \\\"Effect\\\":\\\"Allow\\\",\\r\\n         ");
                permissionPolicy.append(
                                "\\\"Action\\\":[\\r\\n            \\
\"s3:ReplicateObject\\\",\\r\\n            ");
                permissionPolicy
                                .append("\\\"s3:ReplicateDelete\\\",\\r\\n
  \\\"s3:ReplicateTags\\\",\\r\\n            ");
                permissionPolicy.append("\\\"s3:GetObjectVersionTagging\\\"\\r\\n\\r
\\n         ],\\r\\n         ");
                permissionPolicy.append("\\\"Resource\\\":\\\"arn:aws:s3:::");
```

```
                permissionPolicy.append(destinationBucket);
                permissionPolicy.append("/*\\\"\\r\\n      }\\r\\n   ]\\r\\n}");

                PutRolePolicyRequest putRolePolicyRequest = new
 PutRolePolicyRequest()
                                    .withRoleName(roleName)
                                    .withPolicyDocument(permissionPolicy.toString())
                                    .withPolicyName("crrRolePolicy");

                iamClient.putRolePolicy(putRolePolicyRequest);

        }
}
```

C#

L'exemple de AWS SDK pour .NET code suivant ajoute une configuration de réplication à un compartiment, puis la récupère. Pour utiliser ce code, fournissez les noms de vos compartiments et l'Amazon Resource Name (ARN) de votre rôle IAM. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Premiers pas avec le kit AWS SDK pour .NET dans le Guide du développeur AWS SDK pour .NET .

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CrossRegionReplicationTest
    {
        private const string sourceBucket = "*** source bucket ***";
        // Bucket ARN example - arn:aws:s3:::destinationbucket
        private const string destinationBucketArn = "*** destination bucket ARN
 ***";
        private const string roleArn = "*** IAM Role ARN ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint sourceBucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;
        public static void Main()
```

```
        {
            s3Client = new AmazonS3Client(sourceBucketRegion);
            EnableReplicationAsync().Wait();
        }
        static async Task EnableReplicationAsync()
        {
            try
            {
                ReplicationConfiguration replConfig = new ReplicationConfiguration
                {
                    Role = roleArn,
                    Rules =
                        {
                            new ReplicationRule
                            {
                                Prefix = "Tax",
                                Status = ReplicationRuleStatus.Enabled,
                                Destination = new ReplicationDestination
                                {
                                    BucketArn = destinationBucketArn
                                }
                            }
                        }
                };

                PutBucketReplicationRequest putRequest = new
PutBucketReplicationRequest
                {
                    BucketName = sourceBucket,
                    Configuration = replConfig
                };

                PutBucketReplicationResponse putResponse = await
s3Client.PutBucketReplicationAsync(putRequest);

                // Verify configuration by retrieving it.
                await RetrieveReplicationConfigurationAsync(s3Client);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
```

```
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }
        private static async Task RetrieveReplicationConfigurationAsync(IAmazonS3
client)
        {
            // Retrieve the configuration.
            GetBucketReplicationRequest getRequest = new GetBucketReplicationRequest
            {
                BucketName = sourceBucket
            };
            GetBucketReplicationResponse getResponse = await
client.GetBucketReplicationAsync(getRequest);
            // Print.
            Console.WriteLine("Printing replication configuration information...");
            Console.WriteLine("Role ARN: {0}", getResponse.Configuration.Role);
            foreach (var rule in getResponse.Configuration.Rules)
            {
                Console.WriteLine("ID: {0}", rule.Id);
                Console.WriteLine("Prefix: {0}", rule.Prefix);
                Console.WriteLine("Status: {0}", rule.Status);
            }
        }
    }
}
```

Configuration de la réplication pour des compartiments dans des comptes distincts

La réplication dynamique est la copie automatique et asynchrone d'objets dans des compartiments identiques ou différents. Régions AWS La réplication en direct copie les objets nouvellement créés et les mises à jour d'objets à partir d'un compartiment source vers un ou plusieurs compartiments de destination. Pour de plus amples informations, veuillez consulter Réplication d'objets au sein des régions et entre elles.

Lorsque vous configurez la réplication, vous ajoutez des règles de réplication au compartiment source. Les règles de réplication définissent les objets du compartiment source à répliquer, ainsi que le ou les compartiments de destination dans lesquels les objets répliqués seront stockés. Vous pouvez créer une règle pour répliquer tous les objets ou un sous-ensemble d'objets d'un compartiment à l'aide de préfixes de nom de clé ou d'autres balises d'objet, ou les deux. Un

compartiment de destination peut se trouver dans le même compartiment Compte AWS que le compartiment source ou dans un autre compte.

Si vous spécifiez un ID de version d'objet à supprimer, Amazon S3 supprime cette version de l'objet dans le compartiment source. Mais le service ne réplique pas la suppression dans le compartiment de destination. En d'autres termes, il ne supprime pas la même version de l'objet dans le compartiment de destination. Les données sont ainsi protégées contre les suppressions malveillantes.

Lorsque vous ajoutez une règle de réplication à un compartiment, celle-ci est activée par défaut et entre en fonctionnement dès que vous l'enregistrez.

La configuration de la réplication en direct quand les compartiments source et de destination appartiennent à des Comptes AWS différents est similaire à la configuration de la réplication quand les deux compartiments appartiennent au même compte. Toutefois, il existe plusieurs différences lorsque vous configurez la réplication dans un scénario intercompte :

- Le propriétaire du compartiment de destination doit accorder au propriétaire du compartiment source l'autorisation de répliquer des objets dans la politique de compartiment de destination.
- Si vous répliquez des objets chiffrés à l'aide d'un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) dans un scénario intercompte, le propriétaire de la clé KMS doit accorder au propriétaire du compartiment source l'autorisation d'utiliser la clé KMS. Pour de plus amples informations, veuillez consulter Octroi d'autorisations supplémentaires pour les scénarios à plusieurs comptes.
- Par défaut, les objets répliqués appartiennent au propriétaire du compartiment source. Dans un scénario intercompte, vous pouvez configurer la réplication pour remplacer le propriétaire des objets répliqués par le propriétaire du compartiment de destination. Pour de plus amples informations, veuillez consulter Modification du propriétaire d'un réplica.

Pour configurer la réplication lorsque les compartiments source et de destination appartiennent à des entités différentes Comptes AWS

1. Dans cet exemple, vous créez les compartiments source et de destination dans deux Comptes AWS différents. Vous devez avoir défini deux profils d'informations d'identification pour l' AWS CLI. Cet exemple utilise `acctA` et `acctB` pour ces noms de profil. Pour obtenir des informations sur la définition des profils d'informations d'identification et l'utilisation de profils nommés, consultez Paramètres des fichiers de configuration et d'informations d'identification dans le Guide de l'utilisateur AWS Command Line Interface .

2. Suivez les step-by-step instructions en Configuration d'une réplication pour des compartiments dans le même compte apportant les modifications suivantes :

   - Pour toutes les AWS CLI commandes liées aux activités du compartiment source (telles que la création du compartiment source, l'activation du versionnement et la création du rôle IAM), utilisez le `acctA` profil. Utilisez le profil `acctB` pour créer le compartiment de destination.
   - Assurez-vous que la politique d'autorisations pour le rôle IAM spécifie les compartiments source et de destination que vous avez créés pour cet exemple.

3. Dans la console, ajoutez la politique de compartiment suivante au compartiment de destination pour autoriser le propriétaire du compartiment source à répliquer des objets. Pour obtenir des instructions, veuillez consulter Ajout d'une politique de compartiment à l'aide de la console Amazon S3. Veillez à modifier la politique en fournissant l' Compte AWS ID du propriétaire du compartiment source, le nom du rôle IAM et le nom du compartiment de destination.

   > **Note**
   >
   > Pour utiliser l'exemple suivant, remplacez les *`user input placeholders`* par vos propres informations. Remplacez *`amzn-s3-demo-destination-bucket`* par le nom de votre compartiment de destination. Remplacez *`source-bucket-account-ID`*`:role/service-role/`*`source-account-IAM-role`* dans l'Amazon Resource Name (ARN) IAM par le rôle IAM que vous utilisez pour cette configuration de réplication. Si vous avez créé le rôle de service IAM manuellement, définissez le chemin du rôle dans l'ARN IAM sur `role/service-role/`, comme illustré dans l'exemple de politique suivant. Pour plus d'informations, consultez la section IAM ARNs dans le guide de l'utilisateur d'IAM.

   JSON

```
{
    "Version": "2012-10-17",
    "Id": "",
    "Statement": [
        {
            "Sid": "Set-permissions-for-objects",
            "Effect": "Allow",
            "Principal": {
```

```
                "AWS": "arn:aws:iam::111122223333:role/service-role/source-
account-IAM-role"
            },
            "Action": [
                "s3:ReplicateObject",
                "s3:ReplicateDelete"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
        },
        {
            "Sid": "Set permissions on bucket",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::111122223333:role/service-role/source-
account-IAM-role"
            },
            "Action": [
                "s3:GetBucketVersioning",
                "s3:PutBucketVersioning"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
        }
    ]
}
```

4. (Facultatif) Si vous répliquez des objets chiffrés par SSE-KMS, le propriétaire de la clé KMS doit accorder au propriétaire du compartiment source l'autorisation d'utiliser la clé KMS. Pour de plus amples informations, veuillez consulter Octroi d'autorisations supplémentaires pour les scénarios à plusieurs comptes.
5. (Facultatif) Dans une réplication, par défaut, le réplica appartient au propriétaire de l'objet source. Lorsque les compartiments source et de destination appartiennent à des propriétaires différents Comptes AWS, vous pouvez ajouter des paramètres de configuration facultatifs pour remplacer la propriété des répliques par le Compte AWS propriétaire des compartiments de destination. Cela comprend l'octroi de l'autorisation `ObjectOwnerOverrideToBucketOwner`. Pour de plus amples informations, veuillez consulter Modification du propriétaire d'un réplica.

Modification du propriétaire d'un réplica

Dans une réplication, par défaut, le réplica appartient également au propriétaire de l'objet source. Toutefois, lorsque les compartiments source et de destination appartiennent à des propriétaires différents Comptes AWS, vous souhaiterez peut-être modifier le propriétaire de la réplique. Par

exemple, vous pouvez changer l'appartenance afin de limiter l'accès aux réplicas d'objets. Dans votre configuration de réplication, vous pouvez ajouter des paramètres de configuration facultatifs pour remplacer la propriété des répliques par Compte AWS celle qui détient les compartiments de destination.

Pour changer le propriétaire des réplicas, procédez comme suit :

- Ajoutez l'option de substitution du propriétaire à la configuration de réplication pour indiquer à Amazon S3 de modifier le propriétaire des réplicas.
- Accordez à Amazon S3 l'autorisation `s3:ObjectOwnerOverrideToBucketOwner` de modifier le propriétaire des réplicas.
- Ajoutez l'autorisation `s3:ObjectOwnerOverrideToBucketOwner` dans la politique du compartiment de destination pour autoriser la modification du propriétaire des réplicas. L'autorisation `s3:ObjectOwnerOverrideToBucketOwner` permet au propriétaire des compartiments de destination d'accepter la propriété des réplicas d'objet.

Pour plus d'informations, consultez the section called "Considérations relatives à l'option de substitution de propriété" et Ajout de l'option de substitution du propriétaire à la configuration de réplication. Pour un exemple pratique avec des step-by-step instructions, voirComment modifier le propriétaire du réplica.

> **Important**
>
> Au lieu d'utiliser l'option de substitution du propriétaire, vous pouvez utiliser le paramètre appliqué par le propriétaire du compartiment pour Propriété d'objets. Lorsque vous utilisez la réplication et que les compartiments source et de destination appartiennent à des propriétaires différents Comptes AWS, le propriétaire du compartiment de destination peut utiliser le paramètre imposé par le propriétaire du compartiment pour Object Ownership afin de remplacer la propriété de la réplique par le Compte AWS propriétaire du bucket de destination. Ce paramètre désactive les listes de contrôle d'accès aux objets (ACLs). Le paramètre appliqué par le propriétaire du compartiment imite le comportement de substitution de propriétaire existant sans avoir besoin de l'autorisation `s3:ObjectOwnerOverrideToBucketOwner`. Tous les objets répliqués dans le compartiment de destination avec le paramètre Propriétaire du compartiment appliqué appartiennent au propriétaire du compartiment de destination. Pour en savoir plus sur la

propriété des objets, consultez Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Considérations relatives à l'option de substitution de propriété

Lorsque vous configurez l'option de substitution de propriété, les considérations suivantes s'appliquent :

- Par défaut, le propriétaire de l'objet source possède également le réplica. Amazon S3 réplique la version de l'objet et la liste ACL qui lui est associée.

  Si vous ajoutez l'option de substitution de propriétaire à votre configuration de réplication, Amazon S3 réplique uniquement la version de l'objet, mais pas la liste ACL. En outre, Amazon S3 ne réplique pas les modifications ultérieures de la liste ACL de l'objet source. Amazon S3 définit la liste ACL sur le réplica qui accorde un contrôle total au propriétaire du compartiment de destination.
- Lorsque vous mettez à jour une configuration de réplication pour activer ou désactiver la substitution de propriétaire, le comportement suivant intervient :
  - Si vous ajoutez l'option de substitution du propriétaire à la configuration de réplication :

    Quand Amazon S3 réplique une version de l'objet, il supprime la liste ACL associée à l'objet source. Amazon S3 définit à la place la liste ACL sur le réplica et accorde un contrôle total au propriétaire du compartiment de destination. Amazon S3 ne réplique pas les modifications ultérieures de la liste ACL de l'objet source. Toutefois, cette modification de liste de contrôle d'accès (ACL) ne s'applique pas aux versions d'objet répliquées avant la définition de l'option de substitution du propriétaire. Les mises à jour de liste de contrôle d'accès (ACL) pour les objets source répliqués avant la spécification de la substitution du propriétaire continuent donc d'être répliquées (car l'objet et ses réplicas continuent d'avoir le même propriétaire).
  - Si vous supprimez l'option de substitution du propriétaire de la configuration de réplication :

    Amazon S3 réplique les nouveaux objets qui apparaissent dans le compartiment source et dans les compartiments associés ACLs aux compartiments de destination. Pour les objets qui ont été répliqués avant que vous ne supprimiez le remplacement du propriétaire, Amazon S3 ne les réplique pas, ACLs car le changement de propriété de l'objet effectué par Amazon S3 reste en vigueur. En d'autres ACLs termes, la version de l'objet qui a été répliquée lorsque la dérogation par le propriétaire a été définie continue à ne pas être répliquée.

Ajout de l'option de substitution du propriétaire à la configuration de réplication

> **Warning**
>
> Ajoutez l'option de remplacement du propriétaire uniquement lorsque les compartiments source et de destination appartiennent à des propriétaires différents. Comptes AWS Amazon S3 ne vérifie pas si les compartiments appartiennent au même compte ou à des comptes différents. Si vous ajoutez le remplacement du propriétaire alors que les deux compartiments appartiennent au même propriétaire Compte AWS, Amazon S3 applique le remplacement du propriétaire. Cette option accorde des autorisations complètes au propriétaire du compartiment de destination et ne reproduit pas les mises à jour ultérieures des listes de contrôle d'accès des objets sources ()ACLs. Le propriétaire du réplica peut procéder directement à des modifications de la liste de contrôle d'accès (ACL) associée à un réplica à l'aide d'une requête `PutObjectAcl`, mais pas par l'intermédiaire de la réplication.

Pour spécifier l'option de substitution du propriétaire, ajoutez les informations suivantes à chaque élément `Destination` :

- L'élément `AccessControlTranslation`, qui indique à Amazon S3 de modifier le propriétaire des réplicas
- L'`Account`élément, qui indique le propriétaire Compte AWS du compartiment de destination

```
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    ...
    <Destination>
      ...
      <AccessControlTranslation>
           <Owner>Destination</Owner>
       </AccessControlTranslation>
      <Account>destination-bucket-owner-account-id</Account>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

L'exemple de configuration de réplication suivant indique à Amazon S3 de répliquer les objets ayant le préfixe de clé *`Tax`* dans le compartiment de destination *`amzn-s3-demo-destination-`*

bucket et de modifier le propriétaire des réplicas. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <Account>destination-bucket-owner-account-id</Account>
         <AccessControlTranslation>
            <Owner>Destination</Owner>
         </AccessControlTranslation>
      </Destination>
   </Rule>
</ReplicationConfiguration>
```

Octroi à Amazon S3 de l'autorisation de modifier le propriétaire des réplicas

Accordez à Amazon S3 l'autorisation de modifier la propriété de la réplique en ajoutant l'autorisation pour l'`s3:ObjectOwnerOverrideToBucketOwner`action dans la politique d'autorisation associée au rôle AWS Identity and Access Management (IAM). Il s'agit du rôle IAM spécifié dans la configuration de réplication qui autorise Amazon S3 à endosser le rôle et à répliquer les objets en votre nom. Pour utiliser l'exemple suivant, remplacez *amzn-s3-demo-destination-bucket* par le nom du compartiment de destination.

```
...
{
    "Effect":"Allow",
         "Action":[
       "s3:ObjectOwnerOverrideToBucketOwner"
    ],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
```

```
}
...
```

Ajout d'autorisations dans la stratégie du compartiment de destination pour autoriser la modification de propriété du réplica

Le propriétaire du compartiment de destination doit accorder au propriétaire du compartiment source l'autorisation de modifier la propriété du réplica. Le propriétaire du compartiment de destination accorde au propriétaire du compartiment source l'autorisation pour l'action `s3:ObjectOwnerOverrideToBucketOwner`. Cette autorisation permet au propriétaire du compartiment de destination d'accepter la propriété des réplicas d'objet. L'exemple d'instruction de politique de compartiment suivant montre comment procéder. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
...
{
    "Sid":"1",
    "Effect":"Allow",
    "Principal":{"AWS":"source-bucket-account-id"},
    "Action":["s3:ObjectOwnerOverrideToBucketOwner"],
    "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
...
```

Comment modifier le propriétaire du réplica

Lorsque les compartiments source et de destination d'une configuration de réplication appartiennent à des propriétaires différents Comptes AWS, vous pouvez demander à Amazon S3 de remplacer le propriétaire de la réplique par Compte AWS celui qui détient le compartiment de destination. Les exemples suivants montrent comment utiliser la console Amazon S3, le AWS Command Line Interface (AWS CLI) et le AWS SDKs pour modifier le propriétaire de la réplique.

Utilisation de la console S3

Pour step-by-step obtenir des instructions, voirConfiguration d'une réplication pour des compartiments dans le même compte. Cette rubrique fournit des instructions pour configurer une configuration de réplication lorsque les compartiments source et de destination sont détenus de manière identique et différente Comptes AWS.

À l'aide du AWS CLI

La procédure suivante explique comment changer l'appartenance du réplica à l'aide de l' AWS CLI. Dans cette procédure, effectuez les opérations suivantes :

- Créez les compartiments source et de destination.
- Activez la gestion des versions sur ces compartiments.
- Créez un rôle AWS Identity and Access Management (IAM) qui autorise Amazon S3 à répliquer des objets.
- Ajoutez la configuration de réplication au compartiment source.
- Dans la configuration de réplication, vous chargez Amazon S3 de changer l'appartenance du réplica.
- Vous testez votre configuration de réplication.

Pour modifier la propriété de la réplique lorsque les compartiments source et de destination appartiennent à des entités différentes Comptes AWS ()AWS CLI

Pour utiliser les exemples de AWS CLI commandes de cette procédure, remplacez-les *`user input placeholders`* par vos propres informations.

1. Dans cet exemple, vous créez les compartiments source et destination dans deux compartiments différents Comptes AWS. Pour utiliser ces deux comptes, configurez l' AWS CLI avec deux profils nommés. Cet exemple utilise des profils respectivement nommés *`acctA`* et *`acctB`*. Pour obtenir des informations sur la définition des profils d'informations d'identification et l'utilisation de profils nommés, consultez Paramètres des fichiers de configuration et d'informations d'identification dans le Guide de l'utilisateur AWS Command Line Interface .

   > **Important**
   >
   > Les profils que vous utilisez pour cette procédure doivent disposer des autorisations nécessaires. Par exemple, dans la configuration de réplication, vous spécifiez le rôle IAM qu'Amazon S3 peut endosser. Vous ne pouvez effectuer cette tâche que si le profil que vous utilisez dispose de l'autorisation `iam:PassRole`. Si vous utilisez des informations d'identification d'administrateur pour créer un profil nommé, vous pouvez effectuer toutes les tâches de cette procédure. Pour plus d'informations, consultez Octroi d'autorisations

à un utilisateur pour transférer un rôle à un Service AWS dans le Guide de l'utilisateur IAM.

2. Créez le compartiment source et activez la gestion des versions. Cet exemple crée un compartiment source nommé *amzn-s3-demo-source-bucket* dans la région USA Est (Virginie du Nord) (us-east-1).

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. Créez un compartiment de destination et activez la gestion des versions. Cet exemple crée un compartiment de destination nommé *amzn-s3-demo-destination-bucket* dans la région USA Ouest (Oregon) (us-west-2). Utilisez un profil de Compte AWS différent de celui utilisé pour le compartiment source.

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctB
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctB
```

4. Vous devez ajouter des autorisations à la stratégie de votre compartiment de destination pour autoriser la modification de propriété du réplica.

   a. Enregistrez la politique suivante dans un fichier nommé *destination-bucket-policy*.json. Veillez à remplacer les *user input placeholders* par vos propres informations.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "destination_bucket_policy_sid",
            "Principal": {
                "AWS": "source-bucket-owner-account-id"
            },
            "Action": [
                "s3:ReplicateObject",
                "s3:ReplicateDelete",
                "s3:ObjectOwnerOverrideToBucketOwner",
                "s3:ReplicateTags",
                "s3:GetObjectVersionTagging"
            ],
            "Effect": "Allow",
            "Resource": [
                "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
            ]
        }
    ]
}
```

b. Ajoutez la politique précédente au compartiment de destination à l'aide de la commande `put-bucket-policy` suivante :

```
aws s3api put-bucket-policy --region $ {destination-region} --bucket $ {amzn-s3-demo-destination-bucket} --policy file://destination_bucket_policy.json
```

5. Créez un rôle IAM. Vous précisez ce rôle dans la configuration de réplication que vous ajouterez ultérieurement au compartiment source. Amazon S3 endosse ce rôle pour répliquer des objets en votre nom. Vous créez un rôle IAM en deux étapes.

   - Créez le rôle.
   - Attachez une stratégie d'autorisation au rôle.

   a. Créez le rôle IAM.

i. Copiez la stratégie d'approbation suivante et enregistrez-la dans un fichier nommé *s3-role-trust-policy*.json dans le répertoire actif sur votre ordinateur local. Cette stratégie octroie à Amazon S3 les autorisations pour endosser le rôle.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

ii. Exécutez la AWS CLI `create-role` commande suivante pour créer le rôle IAM :

```
$ aws iam create-role \
--role-name replicationRole \
--assume-role-policy-document file://s3-role-trust-policy.json  \
--profile acctA
```

Notez l'Amazon Resource Name (ARN) du rôle IAM que vous avez créé. Vous aurez besoin de cet ARN dans une étape ultérieure.

b. Attachez une stratégie d'autorisation au rôle.

i. Copiez la politique d'autorisations suivante et enregistrez-la dans un fichier nommé *s3-role-perm-pol-changeowner*.json dans le répertoire actuel de votre ordinateur local. Cette stratégie accorde des autorisations pour diverses actions sur les compartiments et les objets Amazon S3. Au cours des étapes suivantes, vous attachez cette politique au rôle IAM que vous avez créé précédemment.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ObjectOwnerOverrideToBucketOwner",
            "s3:ReplicateTags",
            "s3:GetObjectVersionTagging"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      }
   ]
}
```

ii. Pour attacher la politique d'autorisations précédente au rôle, exécutez la commande `put-role-policy` suivante :

```
$ aws iam put-role-policy \
--role-name replicationRole \
--policy-document file://s3-role-perm-pol-changeowner.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

6. Ajoutez une configuration de réplication à votre compartiment source.

   a. AWS CLI Nécessite de spécifier la configuration de réplication au format JSON. Enregistrez la configuration JSON suivante dans un fichier nommé *replication*.json dans le répertoire actif sur votre ordinateur local. Dans cette configuration, AccessControlTranslation spécifie le changement d'appartenance du réplica du propriétaire du compartiment source au propriétaire du compartiment de destination.

```
{
   "Role":"IAM-role-ARN",
   "Rules":[
      {
         "Status":"Enabled",
         "Priority":1,
         "DeleteMarkerReplication":{
            "Status":"Disabled"
         },
         "Filter":{
         },
         "Status":"Enabled",
         "Destination":{
            "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
            "Account":"destination-bucket-owner-account-id",
            "AccessControlTranslation":{
               "Owner":"Destination"
            }
         }
      }
   ]
}
```

   b. Modifiez le code JSON en fournissant des valeurs pour le nom du compartiment de destination, l'ID de compte du propriétaire du compartiment de destination et *IAM-role-ARN*. Remplacez *IAM-role-ARN* par l'ARN du rôle IAM que vous avez créé auparavant. Enregistrez les Modifications.

c. Pour ajouter la configuration de réplication au compartiment source, exécutez la commande suivante :

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

7. Testez votre configuration de réplication en vérifiant l'appartenance du réplica dans la console Amazon S3.

   a. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

   b. Ajoutez des objets au compartiment source. Vérifiez que le compartiment de destination contient les répliques d'objets et que le propriétaire des répliques a été remplacé par Compte AWS celui qui détient le compartiment de destination.

À l'aide du AWS SDKs

Pour obtenir un exemple de code illustrant l'ajout d'une configuration de réplication, consultez À l'aide du AWS SDKs. Vous devez modifier la configuration de réplication en conséquence. Pour obtenir des informations conceptuelles, consultez Modification du propriétaire d'un réplica.

Satisfaction aux exigences de conformité à l'aide du contrôle du temps de réplication S3

Le contrôle du délai de réplication Amazon S3 vous aide à respecter les règles de conformité et les besoins métier en matière de réplication des données, et améliore la visibilité des délais de réplication Amazon S3. S3 RTC réplique la plupart des objets que vous chargez sur Amazon S3 en quelques secondes, et 99,9 % de ces objets en 15 minutes.

Par défaut, le contrôle du temps de réplication S3 inclut deux méthodes pour suivre la progression de la réplication :

- Métriques de réplication S3 : vous pouvez utiliser les métriques de réplication S3 pour surveiller le nombre total d'opérations d'API S3 en attente de réplication, la taille totale des objets en attente de réplication, la durée maximale de réplication vers la région de destination et le nombre total d'opérations pour lesquelles la réplication a échoué. Vous pouvez ensuite surveiller chaque jeu de données que vous répliquez séparément. Vous pouvez également activer les métriques de

réplication S3 indépendamment du contrôle du temps de réplication S3. Pour de plus amples informations, veuillez consulter the section called "Utilisation des métriques de réplication S3".

Les règles de réplication avec le contrôle du temps de réplication S3 (S3 RTC) activé publient des métriques de réplication S3. Les mesures de réplication sont disponibles dans les 15 minutes suivant l'activation de S3 RTC. Les métriques de réplication sont disponibles via la console Amazon S3, l'API Amazon S3 AWS SDKs, the, AWS Command Line Interface the (AWS CLI) et Amazon CloudWatch. Pour plus d'informations sur CloudWatch les métriques, consultezSurveillance des métriques avec Amazon CloudWatch. Pour plus d'informations sur la consultation des métriques de réplication via la console Amazon S3, consultez Affichage des métriques de réplication.

Les métriques de réplication S3 sont facturées au même tarif que les métriques CloudWatch personnalisées d'Amazon. Pour plus d'informations, consultez CloudWatchles tarifs Amazon.

- Notifications d'événement Amazon S3 : le contrôle du temps de réplication S3 fournit des événements `OperationMissedThreshold` et `OperationReplicatedAfterThreshold` qui notifient le propriétaire du compartiment si la réplication d'objet dépasse ou a lieu après le seuil de 15 minutes. Avec le contrôle du temps de réplication S3, les notifications d'événements Amazon S3 peuvent vous avertir dans les rares cas où les objets ne se répliquent pas dans les 15 minutes mais après le seuil de 15 minutes.

  Les événements de réplication sont disponibles dans les 15 minutes suivant l'activation du contrôle du délai de réplication S3. Les notifications d'événements Amazon S3 sont disponibles via Amazon SQS, Amazon SNS ou. AWS Lambda Pour de plus amples informations, veuillez consulter the section called "Réception des événements d'échec de réplication".

Bonnes pratiques et directives de contrôle du délai de réplication S3

Lorsque vous répliquez des données dans Amazon S3 avec le contrôle du temps de réplication S3 (S3 RTC), suivez les directives de ces bonnes pratiques pour optimiser les performances de réplication pour vos charges de travail.

Rubriques

- Directives en matière de performances de réplication et de débit de demandes Amazon S3
- Estimation de vos débits de demandes de réplication
- Dépassement des quotas de débit de transfert de données RTC S3

- AWS KMS taux de demandes de réplication d'objets chiffrés

Directives en matière de performances de réplication et de débit de demandes Amazon S3

Vos applications peuvent exécuter des milliers de transactions par seconde en termes de performances de demande lors du chargement et de la récupération du stockage depuis Amazon S3. Par exemple, une application peut atteindre au moins 3 500 demandes `PUT/COPY/POST/DELETE` ou 5 500 demandes `GET/HEAD` par seconde et par préfixe dans un compartiment S3, y compris les demandes que la réplication S3 effectue en votre nom. Il n'existe aucune limite au nombre de préfixes dans un compartiment. Vous pouvez augmenter vos performances de lecture et d'écriture en effectuant une mise en parallèle des lectures. Par exemple, si vous créez 10 préfixes dans un compartiment S3 pour paralléliser les lectures, vous pouvez mettre à l'échelle vos performances de lecture à 55 000 demandes de lecture par seconde.

Amazon S3 effectue automatiquement une mise à l'échelle en réponse à des débits de demandes soutenus supérieurs à ces directives, ou à des débits de demandes soutenus simultanés à des demandes `LIST`. Tandis qu'Amazon S3 optimise en interne le débit de nouvelles demandes, vous pouvez recevoir temporairement des réponses HTTP 503 jusqu'à ce que l'optimisation soit terminée. Ce comportement peut se produire avec des augmentations des débits de demandes par seconde, ou lorsque vous activez S3 RTC pour la première fois. Au cours de ces périodes, votre latence de réplication peut augmenter. Le contrat de niveau de service (SLA) du contrôle du délai de réplication S3 ne s'applique pas aux périodes où les directives en matière de performances Amazon S3 sur les demandes par seconde sont dépassées.

Le SLA du contrôle du temps de réplication S3 ne s'applique pas non plus pendant les périodes où votre débit de transfert de données de réplication dépasse le quota par défaut de 1 gigabit par seconde (Gbit/s). Si vous pensez que votre débit de transfert de réplication va dépasser 1 Gbit/s, vous pouvez contacter le Centre AWS Support ou utiliser Service Quotas pour demander une augmentation de votre quota de débit de transfert de réplication.

Estimation de vos débits de demandes de réplication

Votre débit de demandes total, y compris les demandes que la réplication Amazon S3 effectue en votre nom, doit être conforme aux directives en matière de débit de demandes Amazon S3 pour les compartiments source et de destination de réplication. Pour chaque objet répliqué, la réplication Amazon S3 effectue jusqu'à cinq demandes `GET/HEAD` et une demande `PUT` vers le compartiment source, ainsi qu'une demande `PUT` vers chaque compartiment de destination.

Par exemple, si vous envisagez de répliquer 100 objets par seconde, la réplication Amazon S3 peut effectuer 100 demandes PUT supplémentaires en votre nom pour un total de 200 demandes PUT par seconde vers le compartiment S3 source. La réplication Amazon S3 peut également effectuer jusqu'à 500 demandes GET/HEAD (5 demandes GET/HEAD pour chaque objet répliqué).

> **Note**
>
> Vous n'engagez des coûts que pour une seule demande PUT par objet répliqué. Pour plus d'informations, consultez les informations tarifaires FAQs sur la réplication dans Amazon S3.

Dépassement des quotas de débit de transfert de données RTC S3

Si vous pensez que votre débit de transfert de données RTC S3 va dépasser le quota par défaut de 1 Gbit/s, contactez le Centre AWS Support ou utilisez Service Quotas pour demander une augmentation de votre quota de débit de transfert de réplication.

AWS KMS taux de demandes de réplication d'objets chiffrés

Lorsque vous répliquez des objets chiffrés avec un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), des quotas de AWS KMS demandes par seconde s'appliquent. AWS KMS peut rejeter une demande par ailleurs valide car votre taux de demandes dépasse le quota du nombre de demandes par seconde. Lorsqu'une demande est limitée, AWS KMS renvoie une `ThrottlingException` erreur. Le quota de taux de AWS KMS demandes s'applique aux demandes que vous effectuez directement et aux demandes effectuées par Amazon S3 Replication en votre nom.

Par exemple, si vous prévoyez de répliquer 1 000 objets par seconde, vous pouvez soustraire 2 000 demandes de votre quota de taux de AWS KMS demandes. Le taux de requêtes par seconde qui en résulte est disponible pour vos AWS KMS charges de travail, à l'exception de la réplication. Vous pouvez utiliser les statistiques des AWS KMS demandes sur Amazon CloudWatch pour surveiller le taux total de AWS KMS demandes sur votre Compte AWS.

Pour demander une augmentation de votre quota de AWS KMS demandes par seconde, contactez AWS Support Center ou utilisez Service Quotas.

Activation du contrôle du délai de réplication S3

Vous pouvez commencer à utiliser le contrôle du délai de réplication S3 avec une règle de réplication nouvelle ou existante. Vous pouvez choisir d'appliquer votre règle de réplication à un compartiment

entier ou à des objets avec un préfixe ou une balise spécifique. Lorsque vous activez S3 RTC, les métriques de réplication S3 sont également activées sur votre règle de réplication.

Vous pouvez configurer S3 RTC à l'aide de la console Amazon S3, de l'API Amazon S3, du AWS SDKs, et du AWS Command Line Interface (AWS CLI).

Utilisation de la console S3

Pour step-by-step obtenir des instructions, voirConfiguration d'une réplication pour des compartiments dans le même compte. Cette rubrique fournit des instructions pour activer S3 RTC dans votre configuration de réplication lorsque les compartiments source et de destination sont détenus de la même manière et de manière différente. Comptes AWS

À l'aide du AWS CLI

AWS CLI Pour répliquer des objets lorsque S3 RTC est activé, vous devez créer des compartiments, activer le contrôle de version sur les compartiments, créer un rôle IAM qui autorise Amazon S3 à répliquer des objets et ajouter la configuration de réplication au compartiment source. La configuration de réplication doit avoir activé S3 RTC, comme illustré dans l'exemple suivant.

Pour step-by-step obtenir des instructions sur la configuration de votre réplication à l'aide du AWS CLI, reportez-vous àConfiguration d'une réplication pour des compartiments dans le même compte.

L'exemple de configuration de réplication suivant active et définit les valeurs `ReplicationTime` et `EventThreshold` pour une règle de réplication. L'activation et la définition de ces valeurs permettent d'activer S3 RTC sur la règle.

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Disabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket",
                "Metrics": {
                    "Status": "Enabled",
                    "EventThreshold": {
```

```
                    "Minutes": 15
                }
            },
            "ReplicationTime": {
                "Status": "Enabled",
                "Time": {
                    "Minutes": 15
                }
            }
        },
        "Priority": 1
    }
  ],
  "Role": "IAM-Role-ARN"
}
```

> **Important**
>
> `Metrics:EventThreshold:Minutes` et `ReplicationTime:Time:Minutes` peuvent uniquement avoir 15 comme valeur valide.

Utilisation du AWS SDK pour Java

Voici un exemple Java permettant d'ajouter une configuration de réplication avec le contrôle du temps de réplication S3 (S3 RTC) activé.

```
import software.amazon.awssdk.auth.credentials.AwsBasicCredentials;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.model.DeleteMarkerReplication;
import software.amazon.awssdk.services.s3.model.Destination;
import software.amazon.awssdk.services.s3.model.Metrics;
import software.amazon.awssdk.services.s3.model.MetricsStatus;
import software.amazon.awssdk.services.s3.model.PutBucketReplicationRequest;
import software.amazon.awssdk.services.s3.model.ReplicationConfiguration;
import software.amazon.awssdk.services.s3.model.ReplicationRule;
import software.amazon.awssdk.services.s3.model.ReplicationRuleFilter;
import software.amazon.awssdk.services.s3.model.ReplicationTime;
import software.amazon.awssdk.services.s3.model.ReplicationTimeStatus;
import software.amazon.awssdk.services.s3.model.ReplicationTimeValue;

public class Main {
```

```
public static void main(String[] args) {
  S3Client s3 = S3Client.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(() -> AwsBasicCredentials.create(
        "AWS_ACCESS_KEY_ID",
        "AWS_SECRET_ACCESS_KEY")
    )
    .build();

  ReplicationConfiguration replicationConfig = ReplicationConfiguration
    .builder()
    .rules(
        ReplicationRule
          .builder()
          .status("Enabled")
          .priority(1)
          .deleteMarkerReplication(
              DeleteMarkerReplication
                  .builder()
                  .status("Disabled")
                  .build()
          )
          .destination(
              Destination
                  .builder()
                  .bucket("destination_bucket_arn")
                  .replicationTime(
                      ReplicationTime.builder().time(
                          ReplicationTimeValue.builder().minutes(15).build()
                      ).status(
                          ReplicationTimeStatus.ENABLED
                      ).build()
                  )
                  .metrics(
                      Metrics.builder().eventThreshold(
                          ReplicationTimeValue.builder().minutes(15).build()
                      ).status(
                          MetricsStatus.ENABLED
                      ).build()
                  )
                  .build()
          )
          .filter(
```

```
                ReplicationRuleFilter
                    .builder()
                    .prefix("testtest")
                    .build()
            )
        .build())
        .role("role_arn")
        .build();

    // Put replication configuration
    PutBucketReplicationRequest putBucketReplicationRequest =
 PutBucketReplicationRequest
      .builder()
      .bucket("source_bucket")
      .replicationConfiguration(replicationConfig)
      .build();

    s3.putBucketReplication(putBucketReplicationRequest);
  }
}
```

Réplication d'objets chiffrés (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C)

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Certaines considérations particulières doivent être prises en compte lorsque vous répliquez des objets qui ont été chiffrés à l'aide du chiffrement côté serveur. Amazon S3 prend en charge les types suivants de chiffrement côté serveur :

- Chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)
- Chiffrement côté serveur avec clés AWS Key Management Service (AWS KMS) (SSE-KMS)
- Chiffrement double couche côté serveur avec AWS KMS clés (DSSE-KMS)
- Chiffrement côté serveur avec clés fournies par le client (SSE-C)

Pour plus d'informations sur le chiffrement côté serveur, consultez the section called "Chiffrement côté serveur".

Cette rubrique explique les autorisations dont vous avez besoin pour demander à Amazon S3 de répliquer des objets qui ont été chiffrés à l'aide du chiffrement côté serveur. Cette rubrique fournit également des éléments de configuration supplémentaires que vous pouvez ajouter, ainsi que des exemples de politiques AWS Identity and Access Management (IAM) qui accordent les autorisations nécessaires pour répliquer des objets chiffrés.

Pour un exemple avec des step-by-step instructions, voirActivation de la réplication pour les objets chiffrés. Pour obtenir des informations sur la création d'une configuration de réplication, consultez Réplication d'objets au sein des régions et entre elles.

> **Note**
>
> Vous pouvez utiliser plusieurs régions AWS KMS keys dans Amazon S3. Cependant, Amazon S3 traite actuellement les clés multi-régions comme s'il s'agissait de clés à région unique et n'utilise pas les fonctions multi-régions de la clé. Pour plus d'informations, consultez Utilisation des clés multi-régions dans le Guide du développeur AWS Key Management Service .

Rubriques

- Comment le chiffrement par défaut du compartiment a un impact sur la réplication
- Réplication d'objets chiffrés avec SSE-C
- Réplication d'objets chiffrés avec SSE-S3, SSE-KMS ou DSSE-KMS
- Activation de la réplication pour les objets chiffrés

Comment le chiffrement par défaut du compartiment a un impact sur la réplication

Après avoir activé le chiffrement par défaut pour un compartiment de destination de réplication, le comportement de chiffrement suivant s'applique :

- Si des objets du compartiment source ne sont pas chiffrés, les objets réplica du compartiment de destination sont chiffrés à l'aide des paramètres de chiffrement par défaut du compartiment de destination. Par conséquent, les étiquettes d'entité (ETags) des objets sources sont différentes de celles ETags des objets répliqués. Si certaines applications l'utilisent ETags, vous devez les mettre à jour pour tenir compte de cette différence.
- Si les objets du compartiment source sont chiffrés à l'aide d'un chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3), d'un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) ou d'un chiffrement double couche côté serveur avec AWS KMS clés (DSSE-KMS), les objets répliques du compartiment de destination utilisent le même type de chiffrement que les objets source. Les paramètres de chiffrement par défaut du compartiment de destination ne sont pas utilisés.

Réplication d'objets chiffrés avec SSE-C

Vous pouvez gérer vos propres clés propriétaires de chiffrement en utilisant un chiffrement côté serveur avec des clés fournies par le client (SSE-C). Avec le SSE-C, vous gérez les clés tandis qu'Amazon S3 gère le processus de chiffrement et de déchiffrement. Vous devez fournir une clé de chiffrement dans le cadre de votre demande, mais vous n'avez pas besoin d'écrire de code pour effectuer le chiffrement ou le déchiffrement d'objets. Lorsque vous chargez un objet, Amazon S3 chiffre l'objet au moyen de la clé que vous avez fournie. Amazon S3 élimine ensuite cette clé de la mémoire. Lorsque vous récupérez un objet, vous devez fournir la même clé de chiffrement dans la demande. Pour de plus amples informations, veuillez consulter the section called "Clés de chiffrement fournies par le client (SSE-C)".

S3 Replication prend en charge les objets chiffrés avec SSE-C. Vous pouvez configurer la réplication d'objets SSE-C dans la console Amazon S3 ou de la AWS SDKs même manière que vous configurez la réplication pour les objets non chiffrés. Il n'existe pas d'autorisations SSE-C supplémentaires au-delà de celles actuellement requises pour la réplication.

La réplication S3 réplique automatiquement les objets chiffrés par SSE-C nouvellement chargés s'ils sont éligibles, conformément à votre configuration de réplication S3. Pour répliquer des objets existants dans vos compartiments, utilisez la réplication par lot S3. Pour plus d'informations sur la

réplication d'objets existants, consultez the section called "Configuration de la réplication en direct" et the section called "Réplication d'objets existants".

La réplication d'objets SSE-C n'entraîne pas de frais supplémentaires. Pour en savoir plus sur la tarification de la réplication, consultez Tarification Amazon S3.

Réplication d'objets chiffrés avec SSE-S3, SSE-KMS ou DSSE-KMS

Par défaut, Amazon S3 ne réplique pas les objets chiffrés avec SSE-KMS ou DSSE-KMS. Cette section explique les éléments de configuration supplémentaire que vous pouvez ajouter de manière à indiquer à Amazon S3 de répliquer ces objets.

Pour un exemple avec des step-by-step instructions, voirActivation de la réplication pour les objets chiffrés. Pour obtenir des informations sur la création d'une configuration de réplication, consultez Réplication d'objets au sein des régions et entre elles.

Spécification d'informations supplémentaires dans la configuration de la réplication

Dans la configuration de réplication, procédez comme suit :

- Dans l'`Destination`élément de votre configuration de réplication, ajoutez l'ID de la clé symétrique gérée par le AWS KMS client que vous souhaitez qu'Amazon S3 utilise pour chiffrer les répliques d'objets, comme illustré dans l'exemple de configuration de réplication suivant.
- Validez explicitement votre choix en activant la réplication d'objets chiffrés avec des clés KMS (SSE-KMS ou DSSE-KMS). Pour valider, ajoutez l'élément `SourceSelectionCriteria`, comme illustré dans l'exemple de configuration de réplication suivant.

```
<ReplicationConfiguration>
   <Rule>
      ...
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
           <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>

      <Destination>
          ...
          <EncryptionConfiguration>
```

```
            <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same
 Région AWS as the destination bucket.</ReplicaKmsKeyID>
         </EncryptionConfiguration>
      </Destination>
      ...
   </Rule>
</ReplicationConfiguration>
```

> **Important**
>
> - La clé KMS doit avoir été créée dans le même compartiment Région AWS que le compartiment de destination.
> - La clé KMS doit être valide. L'opération d'API `PutBucketReplication` ne vérifie pas la validité des clés KMS. Si vous utilisez une clé KMS non valide, vous recevez le code de statut HTTP `200 OK` en réponse, mais la réplication échoue.

L'exemple suivant montre une configuration de réplication qui inclut des éléments de configuration facultatifs. Cette configuration de réplication a une règle. Cette règle s'applique aux objets dotés du préfixe de clé *Tax*. Amazon S3 utilise l' AWS KMS key ID spécifié pour chiffrer ces répliques d'objets.

```
<?xml version="1.0" encoding="UTF-8"?>
<ReplicationConfiguration>
   <Role>arn:aws:iam::account-id:role/role-name</Role>
   <Rule>
      <ID>Rule-1</ID>
      <Priority>1</Priority>
      <Status>Enabled</Status>
      <DeleteMarkerReplication>
         <Status>Disabled</Status>
      </DeleteMarkerReplication>
      <Filter>
         <Prefix>Tax</Prefix>
      </Filter>
      <Destination>
         <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
         <EncryptionConfiguration>
            <ReplicaKmsKeyID>AWS KMS key ARN or Key Alias ARN that's in the same Région
 AWS as the destination bucket.</ReplicaKmsKeyID>
         </EncryptionConfiguration>
      </Destination>
```

```
      <SourceSelectionCriteria>
         <SseKmsEncryptedObjects>
            <Status>Enabled</Status>
         </SseKmsEncryptedObjects>
      </SourceSelectionCriteria>
   </Rule>
</ReplicationConfiguration>
```

Octroi d'autorisations supplémentaires pour le rôle IAM

Pour répliquer des objets chiffrés au repos à l'aide de SSE-S3, SSE-KMS ou DSSE-KMS, accordez les autorisations supplémentaires suivantes au rôle AWS Identity and Access Management (IAM) que vous spécifiez dans la configuration de réplication. Vous octroyez ces autorisations en mettant à jour la stratégie d'autorisations associée au rôle IAM.

- Action **`s3:GetObjectVersionForReplication`** pour les objets sources – Cette action permet à Amazon S3 de répliquer les objets non chiffrés et les objets créés avec un chiffrement côté serveur en utilisant une clé SSE-S3, SSE-KMS ou DSSE-KMS.

  > **Note**
  >
  > Nous vous recommandons d'utiliser l'action `s3:GetObjectVersionForReplication` à la place de l'action `s3:GetObjectVersion`, car `s3:GetObjectVersionForReplication` fournit uniquement à Amazon S3 le minimum d'autorisations nécessaires pour la réplication. De plus, l'action `s3:GetObjectVersion` permet la réplication des objets non chiffrés et des objets chiffrés avec SSE-S3, mais pas la réplication des objets chiffrés avec des clés KMS (SSE-KMS ou DSSE-KMS).

- **`kms:Decrypt`**et **`kms:Encrypt`** AWS KMS actions pour les clés KMS
  - Vous devez accorder des autorisations `kms:Decrypt` pour l' AWS KMS key utilisée pour déchiffrer l'objet source.
  - Vous devez accorder des autorisations `kms:Encrypt` pour la AWS KMS key utilisée pour chiffrer le réplica source.
- Action **`kms:GenerateDataKey`** pour la réplication d'objets en texte brut – Si vous répliquez des objets en texte brut dans un compartiment avec le chiffrement SSE-KMS ou DSSE-KMS activé par défaut, vous devez inclure l'autorisation `kms:GenerateDataKey` pour le contexte de chiffrement de destination et la clé KMS dans la politique IAM.

Nous vous recommandons de limiter ces autorisations uniquement aux compartiments et objets de destination en utilisant des clés de AWS KMS condition. Le Compte AWS titulaire du rôle IAM doit disposer d'autorisations `kms:Encrypt` et d'`kms:Decrypt`actions pour les clés KMS répertoriées dans la politique. Si les clés KMS appartiennent à une autre personne Compte AWS, le propriétaire des clés KMS doit accorder ces autorisations au Compte AWS titulaire du rôle IAM. Pour plus d'informations sur la gestion de l'accès à ces clés KMS, consultez la section Utilisation des politiques IAM AWS KMS dans le Guide du AWS Key Management Service développeur.

Clés de compartiment S3 et réplication

Pour utiliser la réplication avec une clé de compartiment S3, la AWS KMS key politique relative à la clé KMS utilisée pour chiffrer la réplique de l'objet doit inclure l'`kms:Decrypt`autorisation du principal appelant. L'appel à `kms:Decrypt` vérifie l'intégrité de la clé de compartiment S3 avant de l'utiliser. Pour plus d'informations, consultez Utilisation d'une clé de compartiment S3 avec réplication.

Lorsqu'une clé de compartiment S3 est activée pour le compartiment source ou de destination, le contexte de chiffrement est l'Amazon Resource Name (ARN) du compartiment et non l'ARN de l'objet (par exemple, `arn:aws:s3:::`*`bucket_ARN`*). Vous devez mettre à jour vos politiques IAM pour utiliser l'ARN du compartiment pour le contexte de chiffrement :

```
"kms:EncryptionContext:aws:s3:arn": [
"arn:aws:s3:::bucket_ARN"
]
```

Pour plus d'informations, consultez Contexte de chiffrement (`x-amz-server-side-encryption-context`) (dans la section « Utilisation de l'API REST ») et Modifications à prendre en compte avant d'activer une clé de compartiment S3.

Exemples de politiques : utilisation de SSE-S3 et de SSE-KMS avec la réplication

L'exemple suivant de politiques IAM montre des instructions pour l'utilisation du SSE-S3 et du SSE-KMS avec la réplication.

Example : utilisation de SSE-KMS avec des compartiments de destination distincts

L'exemple suivant de politique présente des instructions pour l'utilisation du SSE-KMS avec des compartiments de destination distincts.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action": ["kms:Decrypt"],
         "Effect": "Allow",
         "Condition": {
             "StringLike": {
                  "kms:ViaService": "s3.source-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn": [
                      "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
                  ]
             }
          },
          "Resource": [
             "List of AWS KMS key ARNs that are used to encrypt source objects."
          ]
      },
      {
         "Action": ["kms:Encrypt"],
         "Effect": "Allow",
         "Condition": {
            "StringLike": {
               "kms:ViaService": "s3.destination-bucket-1-region.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn": [
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket1/key-prefix1*"
               ]
         }
         },
         "Resource": [
            "AWS KMS key ARNs (in the same Région AWS example-region; as
 destination bucket 1). Used to encrypt object replicas created in destination
 bucket 1."
         ]
      },
      {
         "Action": ["kms:Encrypt"],
         "Effect": "Allow",
         "Condition": {
            "StringLike": {
               "kms:ViaService": "s3.destination-bucket-2-region.amazonaws.com",
```

```
                "kms:EncryptionContext:aws:s3:arn": [
                   "arn:aws:s3:::amzn-s3-demo-destination-bucket2/key-prefix1*"
                ]
            }
            },
            "Resource": [
               "AWS KMS key ARNs (in the same Région AWS example-region; as
 destination bucket 2). Used to encrypt object replicas created in destination
 bucket 2."
            ]
        }
    ]
}
```

Example : réplication d'objets créés avec SSE-S3 et SSE-KMS

Vous trouverez ci-dessous une politique IAM complète qui accorde les autorisations nécessaires pour répliquer des objets non chiffrés, des objets créés avec le SSE-S3 et des objets créés avec le SSE-KMS.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
```

```
            "Resource":[
               "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
            ]
         },
         {
            "Effect":"Allow",
            "Action":[
               "s3:ReplicateObject",
               "s3:ReplicateDelete"
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
         },
         {
            "Action":[
               "kms:Decrypt"
            ],
            "Effect":"Allow",
            "Condition":{
               "StringLike":{
                  "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn":[
                     "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
                  ]
               }
            },
            "Resource":[
              "List of the AWS KMS key ARNs that are used to encrypt source
    objects."
            ]
         },
         {
            "Action":[
               "kms:Encrypt"
            ],
            "Effect":"Allow",
            "Condition":{
               "StringLike":{
                  "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn":[
                     "arn:aws:s3:::amzn-s3-demo-destination-bucket/prefix1*"
                  ]
               }
            },
            "Resource":[
```

```
            "AWS KMS key ARNs (in the same aws-region as the destination bucket)
 to use for encrypting object replicas"
         ]
      }
   ]
}
```

Example : réplication d'objets avec des clés de compartiment S3

Voici une politique IAM complète qui accorde les autorisations nécessaires pour répliquer des objets avec des clés de compartiment S3.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:ListBucket"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/key-prefix1*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete"
```

```
            ],
            "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/key-prefix1*"
        },
        {
            "Action":[
               "kms:Decrypt"
            ],
            "Effect":"Allow",
            "Condition":{
               "StringLike":{
                  "kms:ViaService":"s3.source-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn":[
                     "arn:aws:s3:::amzn-s3-demo-source-bucket"
                  ]
               }
            },
            "Resource":[
              "List of the AWS KMS key ARNs that are used to encrypt source
 objects."
            ]
        },
        {
            "Action":[
               "kms:Encrypt"
            ],
            "Effect":"Allow",
            "Condition":{
               "StringLike":{
                  "kms:ViaService":"s3.destination-bucket-region.amazonaws.com",
                  "kms:EncryptionContext:aws:s3:arn":[
                     "arn:aws:s3:::amzn-s3-demo-destination-bucket"
                  ]
               }
            },
            "Resource":[
               "AWS KMS key ARNs (in the same aws-region as the destination bucket)
 to use for encrypting object replicas"
            ]
        }
    ]
}
```

Octroi d'autorisations supplémentaires pour les scénarios à plusieurs comptes

Dans un scénario entre comptes, dans lequel les compartiments source et destination sont détenus par des entités différentes Comptes AWS, vous pouvez utiliser une clé KMS pour chiffrer les répliques d'objets. Le propriétaire de la clé KMS doit accorder au propriétaire du compartiment source l'autorisation d'utiliser la clé KMS.

> **Note**
>
> Si vous devez répliquer des données SSE-KMS entre comptes, votre règle de réplication doit spécifier une clé gérée par le client AWS KMS pour le compte de destination. Clés gérées par AWSn'autorisent pas l'utilisation entre comptes et ne peuvent donc pas être utilisés pour effectuer une réplication entre comptes.

Pour accorder au propriétaire du compartiment source l'autorisation d'utiliser la clé KMS (console AWS KMS)

1. Connectez-vous à la AWS KMS console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/km.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
3. Pour afficher les clés de votre compte que vous créez et gérez vous-même, dans le volet de navigation, choisissez Clés gérées par le client.
4. Sélectionnez la clé KMS.
5. Sous la section Configuration générale, choisissez l'onglet Stratégie de clé.
6. Faites défiler la page vers le bas jusqu'à Autre Comptes AWS.
7. Choisissez Ajouter un autre Comptes AWS.

   La boîte de dialogue Autres Comptes AWS s'affiche.
8. Dans la boîte de dialogue, choisissez Ajouter un autre Compte AWS. Pour arn:aws:iam::, saisissez l'ID de compte du compartiment source.
9. Sélectionnez Enregistrer les modifications.

Pour octroyer au propriétaire du compartiment source l'autorisation d'utiliser la clé KMS (AWS CLI)

- Pour plus d'informations sur la commande `put-key-policy` AWS Command Line Interface (AWS CLI), reportez-vous put-key-policyà la référence des AWS CLI commandes. Pour plus d'informations sur l'opération d'API `PutKeyPolicy` sous-jacente, consultez PutKeyPolicy dans la Référence d'API AWS Key Management Service.

AWS KMS considérations relatives aux quotas de transactions

Lorsque vous ajoutez de nombreux nouveaux objets AWS KMS chiffrés après avoir activé la réplication entre régions (CRR), vous pouvez rencontrer un ralentissement (erreurs HTTP). `503 Service Unavailable` La limitation survient lorsque le nombre de transactions AWS KMS par seconde dépasse le quota actuel. Pour plus d'informations, consultez Quotas dans le Guide du développeur AWS Key Management Service .

Pour demander l'augmentation d'un quota, utilisez Service Quotas. Pour plus d'informations, consultez Demande d'augmentation de quota. Si le Service Quotas n'est pas pris en charge dans votre région, ouvrez un AWS Support dossier.

Activation de la réplication pour les objets chiffrés

Par défaut, Amazon S3 ne réplique pas les objets chiffrés à l'aide d'un chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) ou d'un chiffrement double couche côté serveur avec clés (DSSE-KMS). AWS KMS Pour répliquer des objets chiffrés avec SSE-KMS ou DSS-KMS, vous devez modifier la configuration de réplication des compartiments de façon à demander à Amazon S3 de répliquer ces objets. Cet exemple explique comment utiliser la console Amazon S3 et le AWS Command Line Interface (AWS CLI) pour modifier la configuration de réplication du compartiment afin de permettre la réplication d'objets chiffrés.

> **Note**
>
> Lorsqu'une clé de compartiment S3 est activée pour le compartiment source ou de destination, le contexte de chiffrement est l'Amazon Resource Name (ARN) du compartiment et non l'ARN de l'objet. Vous devez mettre à jour vos politiques IAM pour utiliser l'ARN du compartiment pour le contexte de chiffrement. Pour de plus amples informations, veuillez consulter Clés de compartiment S3 et réplication.

> **Note**
>
> Vous pouvez utiliser plusieurs régions AWS KMS keys dans Amazon S3. Cependant, Amazon S3 traite actuellement les clés multi-régions comme s'il s'agissait de clés à région unique et n'utilise pas les fonctions multi-régions de la clé. Pour plus d'informations, consultez Utilisation des clés multi-régions dans le Guide du développeur AWS Key Management Service .

Utilisation de la console S3

Pour step-by-step obtenir des instructions, voirConfiguration d'une réplication pour des compartiments dans le même compte. Cette rubrique fournit des instructions pour définir une configuration de réplication lorsque les compartiments source et de destination sont détenus de manière identique et différente Comptes AWS.

À l'aide du AWS CLI

Pour répliquer des objets chiffrés avec le AWS CLI, procédez comme suit :

- Créez les compartiments source et de destination et activez la gestion des versions pour ces mêmes compartiments.
- Créez un rôle de service AWS Identity and Access Management (IAM) qui autorise Amazon S3 à répliquer des objets. Les autorisations accordées au rôle IAM incluent les autorisations nécessaires à la réplication des objets chiffrés.
- Ajoutez une configuration de réplication au compartiment source. La configuration de réplication fournit des informations sur la réplication des objets chiffrés à l'aide de clés KMS.
- Ajoutez des objets chiffrés au compartiment source.
- Testez la configuration pour vérifier que vos objets chiffrés sont répliqués dans le compartiment de destination.

Les procédures suivantes vous guident tout au long de ce processus.

Pour répliquer des objets chiffrés côté serveur (AWS CLI)

Pour utiliser les exemples de cette procédure, remplacez les *`user input placeholders`* par vos propres informations.

1. Dans cet exemple, vous créez à la fois les compartiments source (*amzn-s3-demo-source-bucket*) et de destination (*amzn-s3-demo-destination-bucket*) dans le même Compte AWS. Vous allez également définir un profil d'informations d'identification pour l' AWS CLI. Cet exemple utilise le nom de profil *acctA*.

   Pour obtenir des informations sur la définition des profils d'informations d'identification et l'utilisation de profils nommés, consultez Paramètres des fichiers de configuration et d'informations d'identification dans le Guide de l'utilisateur AWS Command Line Interface .

2. Utilisez les commandes suivantes pour créer le compartiment *amzn-s3-demo-source-bucket* et activer la gestion des versions sur celui-ci. Les commandes de l'exemple suivant créent le compartiment *amzn-s3-demo-source-bucket* dans la région USA Est (Virginie du Nord) (`us-east-1`).

```
aws s3api create-bucket \
--bucket amzn-s3-demo-source-bucket \
--region us-east-1 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-source-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

3. Utilisez les commandes suivantes pour créer le compartiment *amzn-s3-demo-destination-bucket* et activer la gestion des versions sur celui-ci. Les commandes de l'exemple suivant créent le compartiment *amzn-s3-demo-destination-bucket* dans la région USA Ouest (Oregon) (`us-west-2`).

> **Note**
>
> Pour définir une configuration de réplication lorsque les compartiments *amzn-s3-demo-source-bucket* et *amzn-s3-demo-destination-bucket* se trouvent dans le même Compte AWS, utilisez le même profil. Cet exemple utilise *acctA*. Pour configurer la réplication lorsque les buckets appartiennent à des propriétaires différents Comptes AWS, vous devez spécifier des profils différents pour chacun d'entre eux.

```
aws s3api create-bucket \
--bucket amzn-s3-demo-destination-bucket \
--region us-west-2 \
--create-bucket-configuration LocationConstraint=us-west-2 \
--profile acctA
```

```
aws s3api put-bucket-versioning \
--bucket amzn-s3-demo-destination-bucket \
--versioning-configuration Status=Enabled \
--profile acctA
```

4. Ensuite, créez un rôle de service IAM. Vous allez spécifier ce rôle dans la configuration de réplication que vous ajouterez ultérieurement au compartiment *amzn-s3-demo-source-bucket*. Amazon S3 endosse ce rôle pour répliquer des objets en votre nom. Vous créez un rôle IAM en deux étapes.

   - Créez un rôle de service.
   - Attachez une stratégie d'autorisation au rôle.

   a. Pour créer un rôle de service IAM, procédez comme suit :

      i. Copiez la stratégie d'approbation suivante et enregistrez-la dans un fichier nommé *s3-role-trust-policy-kmsobj*`.json` dans le répertoire actif sur votre ordinateur local. Cette politique accorde au principal de service Amazon S3 les autorisations nécessaires pour endosser le rôle et permettre ainsi à Amazon S3 d'effectuer des tâches en votre nom.

      JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
```

```
      }
   ]
}
```

ii. Utilisez la commande suivante pour créer le rôle :

```
$ aws iam create-role \
--role-name replicationRolekmsobj \
--assume-role-policy-document file://s3-role-trust-policy-kmsobj.json  \
--profile acctA
```

b. Ensuite, attachez une stratégie d'autorisation au rôle. Cette stratégie accorde des autorisations pour diverses actions sur les compartiments et les objets Amazon S3.

i. Copiez la politique d'autorisations suivante et enregistrez-la dans un fichier nommé *s3-role-permissions-policykmsobj*.json dans le répertoire actuel de votre ordinateur local. Vous allez créer un rôle IAM et attacherez par la suite la stratégie à celui-ci.

> **Important**
>
> Dans la politique d'autorisation, vous spécifiez la AWS KMS clé IDs qui sera utilisée pour le chiffrement des *amzn-s3-demo-destination-bucket* compartiments *amzn-s3-demo-source-bucket* et. Vous devez créer deux clés KMS distinctes pour les *amzn-s3-demo-destination-bucket* compartiments *amzn-s3-demo-source-bucket* et. AWS KMS keys ne sont pas partagés en dehors de Région AWS celui dans lequel ils ont été créés.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:ListBucket",
            "s3:GetReplicationConfiguration",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
```

```
            "s3:GetObjectVersionTagging"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket",
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLikeIfExists":{
               "s3:x-amz-server-side-encryption":[
                  "aws:kms",
                  "AES256",
                  "aws:kms:dsse"
               ],
               "s3:x-amz-server-side-encryption-aws-kms-key-id":[
                  "AWS KMS key IDs(in ARN format) to use for
encrypting object replicas"
               ]
            }
         },
         "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
      },
      {
         "Action":[
            "kms:Decrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.us-east-1.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
               ]
            }
         },
         "Resource":[
```

```
            "arn:aws:kms:us-east-1:111122223333:key/key-id"
         ]
      },
      {
         "Action":[
            "kms:Encrypt"
         ],
         "Effect":"Allow",
         "Condition":{
            "StringLike":{
               "kms:ViaService":"s3.us-west-2.amazonaws.com",
               "kms:EncryptionContext:aws:s3:arn":[
                  "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
               ]
            }
         },
         "Resource":[
            "arn:aws:kms:us-west-2:111122223333:key/key-id"
         ]
      }
   ]
}
```

ii. Créez une politique et attachez-la au rôle.

```
$ aws iam put-role-policy \
--role-name replicationRolekmsobj \
--policy-document file://s3-role-permissions-policykmsobj.json \
--policy-name replicationRolechangeownerPolicy \
--profile acctA
```

5. Ensuite, ajoutez la configuration de réplication suivante au compartiment *amzn-s3-demo-source-bucket*. Elle demande à Amazon S3 de répliquer les objets dotés du préfixe *Tax/* dans le compartiment *amzn-s3-demo-destination-bucket*.

> **Important**
>
> Dans la configuration de réplication, spécifiez le rôle IAM qu'Amazon S3 peut endosser. Vous ne pouvez effectuer cette tâche que si vous disposez de l'autorisation `iam:PassRole`. Le profil que vous spécifiez dans la commande CLI doit disposer

de cette autorisation. Pour plus d'informations, consultez Octroi d'autorisations à un utilisateur pour transférer un rôle à un Service AWS dans le Guide de l'utilisateur IAM.

```
 <ReplicationConfiguration>
  <Role>IAM-Role-ARN</Role>
  <Rule>
    <Priority>1</Priority>
    <DeleteMarkerReplication>
       <Status>Disabled</Status>
    </DeleteMarkerReplication>
    <Filter>
       <Prefix>Tax</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <SourceSelectionCriteria>
      <SseKmsEncryptedObjects>
        <Status>Enabled</Status>
      </SseKmsEncryptedObjects>
    </SourceSelectionCriteria>
    <Destination>
      <Bucket>arn:aws:s3:::amzn-s3-demo-destination-bucket</Bucket>
      <EncryptionConfiguration>
        <ReplicaKmsKeyID>AWS KMS key IDs to use for encrypting object replicas</
ReplicaKmsKeyID>
      </EncryptionConfiguration>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

Pour ajouter une configuration de réplication au compartiment *amzn-s3-demo-source-bucket*, procédez comme suit :

a. Vous AWS CLI devez spécifier la configuration de réplication au format JSON. Enregistrez la configuration JSON suivante dans un fichier (*replication*.json) dans le répertoire actuel sur votre ordinateur local.

```
{
   "Role":"IAM-Role-ARN",
   "Rules":[
      {
```

```
            "Status":"Enabled",
            "Priority":1,
            "DeleteMarkerReplication":{
               "Status":"Disabled"
            },
            "Filter":{
               "Prefix":"Tax"
            },
            "Destination":{
               "Bucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
               "EncryptionConfiguration":{
                  "ReplicaKmsKeyID":"AWS KMS key IDs (in ARN format) to use for
 encrypting object replicas"
               }
            },
            "SourceSelectionCriteria":{
               "SseKmsEncryptedObjects":{
                  "Status":"Enabled"
               }
            }
         }
      ]
}
```

b. Modifiez le JSON pour indiquer les valeurs du compartiment *amzn-s3-demo-destination-bucket*, des *AWS KMS key IDs (in ARN format)* et de l'*IAM-role-ARN*. Enregistrez les Modifications.

c. Utilisez la commande suivante pour ajouter la configuration de réplication à votre compartiment *amzn-s3-demo-source-bucket*. Veillez à saisir le nom du compartiment *amzn-s3-demo-source-bucket*.

```
$ aws s3api put-bucket-replication \
--replication-configuration file://replication.json \
--bucket amzn-s3-demo-source-bucket \
--profile acctA
```

6. Testez la configuration pour vérifier que les objets chiffrés ont été répliqués. Dans la console Amazon S3, procédez comme suit :

a. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

b. Dans le compartiment *amzn-s3-demo-source-bucket*, créez un dossier nommé *Tax*.

c. Ajoutez des exemples d'objet au dossier. Assurez-vous de choisir l'option de chiffrement et de spécifier votre clé KMS pour chiffrer les objets.

d. Vérifiez que le compartiment *amzn-s3-demo-destination-bucket* contient les réplicas d'objets et qu'ils ont été chiffrés avec la clé KMS que vous avez spécifiée dans la configuration. Pour de plus amples informations, veuillez consulter the section called "Obtention du statut de réplication".

À l'aide du AWS SDKs

Pour obtenir un exemple de code montrant comment ajouter une configuration de réplication, consultez À l'aide du AWS SDKs. Vous devez modifier la configuration de réplication en conséquence.

Réplication des modifications des métadonnées avec la synchronisation des modifications de réplica

La synchronisation des modifications des répliques Amazon S3 peut vous aider à conserver les métadonnées des objets telles que les balises, les listes de contrôle d'accès (ACLs) et les paramètres de verrouillage des objets répliquées entre les répliques et les objets source. Par défaut, Amazon S3 réplique les métadonnées des objets source vers les réplicas uniquement. Lorsque la synchronisation des modifications de réplica est activée, Amazon S3 réplique les modifications de métadonnées apportées aux copies de réplica vers l'objet source, ce qui rend la réplication bidirectionnelle.

Activer de la synchronisation des modifications de réplica

Vous pouvez utiliser la synchronisation des modifications de réplica Amazon S3 avec des règles de réplication nouvelles ou existantes. Vous pouvez l'appliquer à un compartiment entier ou à des objets qui ont un préfixe spécifique.

Pour activer la synchronisation des modifications de réplica à l'aide de la console Amazon S3, consultez Exemples de configuration de la réplication en direct. Cette rubrique fournit des instructions pour activer la synchronisation des modifications des répliques dans votre configuration de réplication lorsque les compartiments source et de destination appartiennent à des entités identiques ou différentes Comptes AWS.

Pour activer la synchronisation des modifications des répliques à l'aide de AWS Command Line Interface (AWS CLI), vous devez ajouter une configuration de réplication au compartiment contenant les répliques `ReplicaModifications` activées. Pour configurer la réplication bidirectionnelle,

créez une règle de réplication à partir du compartiment source (*amzn-s3-demo-source-bucket*) vers le compartiment contenant les réplicas (*amzn-s3-demo-destination-bucket*). Ensuite, créez une seconde règle de réplication à partir du compartiment contenant les réplicas (*amzn-s3-demo-destination-bucket*) vers le compartiment source (*amzn-s3-demo-source-bucket*). Les compartiments source et destination peuvent être identiques ou différents Régions AWS.

> **Note**
>
> Vous devez activer la synchronisation des modifications des répliques sur les compartiments source et de destination pour répliquer les modifications des métadonnées des répliques, telles que les listes de contrôle d'accès aux objets (ACLs), les balises d'objets ou les paramètres de verrouillage des objets sur les objets répliqués. Comme toutes les règles de réplication, vous pouvez appliquer ces règles à l'ensemble du compartiment ou à un sous-ensemble d'objets filtrés par un préfixe ou des balises d'objet.

Dans l'exemple de configuration suivant, Amazon S3 réplique les modifications de métadonnées sous le préfixe *Tax* dans le compartiment *amzn-s3-demo-source-bucket*, qui contient les objets sources.

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "SourceSelectionCriteria": {
                "ReplicaModifications":{
                    "Status": "Enabled"
                }
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-source-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

Pour obtenir des instructions complètes sur la création de règles de réplication à l'aide du AWS CLI, voirConfiguration d'une réplication pour des compartiments dans le même compte.

Répliquer des marqueurs de suppression entre les compartiments

Par défaut, lorsque la réplication S3 est activée et qu'un objet est supprimé dans le compartiment source, Amazon S3 ajoute un marqueur de suppression dans le compartiment source uniquement. Cette action aide à protéger les données dans les compartiments de destination contre les suppressions accidentelles ou malveillantes. Si la réplication des marqueurs de suppression est activée, ces marqueurs sont copiés dans les compartiments de destination et Amazon S3 se comporte comme si l'objet avait été supprimé dans les compartiments source et de destination. Pour plus d'informations sur le fonctionnement des marqueurs de suppression, consultez Utilisation des marqueurs de suppression.

> **Note**
>
> - La réplication des marqueurs de suppression n'est pas prise en charge pour les règles de réplication basées sur des balises. La réplication des marqueurs de suppression ne respecte pas non plus le contrat de niveau de service (SLA) de 15 minutes convenu pour l'utilisation du contrôle du temps de réplication S3 (S3 RTC).
> - Si vous n'utilisez pas la dernière version XML de configuration de réplication, les opérations de suppression affectent la réplication différemment. Pour de plus amples informations, veuillez consulter Impact des opérations de suppression sur la réplication.
> - Si vous activez la réplication des marqueurs de suppression et que votre compartiment source possède une règle d'expiration du cycle de vie S3, les marqueurs de suppression ajoutés par la règle d'expiration du cycle de vie S3 ne seront pas répliqués dans le compartiment de destination.

Activer la réplication des marqueurs de suppression

Vous pouvez commencer à utiliser la réplication des marqueurs de suppression avec une règle de réplication nouvelle ou existante. Vous pouvez appliquer la réplication des marqueurs de suppression à un compartiment entier ou à des objets dotés d'un préfixe spécifique.

Pour activer la réplication des marqueurs de suppression à l'aide de la console Amazon S3, consultez Utilisation de la console S3. Cette rubrique fournit des instructions pour activer la réplication des marqueurs de suppression dans votre configuration de réplication lorsque les

compartiments source et de destination appartiennent à la même personne ou à des entités différentes Comptes AWS.

Pour activer la réplication des marqueurs de suppression à l'aide de AWS Command Line Interface (AWS CLI), vous devez ajouter une configuration de réplication au compartiment source en `DeleteMarkerReplication` activant, comme indiqué dans l'exemple de configuration suivant.

Dans l'exemple de configuration de réplication suivant, les marqueurs de suppression sont répliqués dans le compartiment de destination *`amzn-s3-demo-destination-bucket`* pour les objets sous le préfixe *`Tax`*.

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "DeleteMarkerReplication": {
                "Status": "Enabled"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-destination-bucket"
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

Pour obtenir des instructions complètes sur la création de règles de réplication par le biais du AWS CLI, voirConfiguration d'une réplication pour des compartiments dans le même compte.

Gestion ou suspension de la réplication en direct

La réplication dynamique est la copie automatique et asynchrone d'objets dans des compartiments identiques ou différents. Régions AWS Une fois que vous avez défini votre configuration de réplication, Amazon S3 réplique les objets nouvellement créés et les mises à jour d'objets à partir d'un compartiment source vers un ou plusieurs compartiments de destination spécifiés.

Utilisez la console Amazon S3 pour ajouter des règles de réplication dans le compartiment source. Les règles de réplication définissent les objets du compartiment source à répliquer, ainsi que le

compartiment de destination dans lequel les objets répliqués seront stockés. Pour plus d'informations sur la réplication, consultez Réplication d'objets au sein des régions et entre elles.

Vous pouvez gérer les règles de réplication sur la page Réplication dans la console Amazon S3. Vous pouvez ajouter, afficher, modifier, activer, désactiver ou supprimer des règles de réplication. Vous pouvez également modifier la priorité de vos règles de réplication. Pour plus d'informations sur l'ajout de règles de réplication à un compartiment, consultez Utilisation de la console S3.

Pour gérer les règles de réplication pour un compartiment à l'aide de la console Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans l'onglet Compartiments à usage général, choisissez le nom du compartiment que vous souhaitez utiliser.
4. Choisissez l'onglet Gestion, puis faites défiler jusqu'à Règles de réplication.
5. Vous pouvez modifier vos règles de réplication des manières suivantes :
   - Pour activer ou désactiver une règle de réplication, sélectionnez la case d'option située à gauche de la règle. Dans le menu Actions, choisissez Activer la règle ou Désactiver la règle. Vous pouvez également désactiver, activer ou supprimer toutes les règles du compartiment à partir du menu Actions.

     > **Note**
     >
     > Si vous désactivez une règle de réplication puis la réactivez ultérieurement, les objets nouveaux ou modifiés qui n'ont pas été répliqués lorsque la règle était désactivée ne sont pas automatiquement répliqués lors de la réactivation de la règle. Pour répliquer ces objets, vous devez utiliser la réplication par lot S3. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets existants".

   - Pour modifier la priorité d'une règle, sélectionnez la case d'option située à gauche de la règle, puis choisissez Modifier la règle.

     Vous devez définir les priorités des règles pour éviter les conflits provoqués par les objets inclus dans l'étendue de plusieurs règles. En cas de chevauchement de règles, Amazon S3 utilise la priorité des règles pour déterminer la règle à appliquer. Plus le nombre est élevé,

plus la priorité est haute. Pour plus d'informations sur la priorité des règles, consultez Éléments du fichier de configuration de réplication.

Suspension ou arrêt de la réplication

Pour suspendre temporairement la réplication et la reprendre automatiquement ultérieurement, vous pouvez utiliser l'action `aws:s3:bucket-pause-replication` dans AWS Fault Injection Service. Pour plus d'informations, consultez aws:s3:bucket-pause-replication et Suspendre la réplication S3 dans le Guide de l'utilisateur AWS Fault Injection Service .

Pour arrêter la réplication dans Amazon S3, nous vous recommandons de désactiver vos règles de réplication. Si vous désactivez une règle de réplication puis la réactivez ultérieurement, les objets nouveaux ou modifiés qui n'ont pas été répliqués lorsque la règle était désactivée ne sont pas automatiquement répliqués lors de la réactivation de la règle. Pour répliquer ces objets, vous devez utiliser la réplication par lot S3. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets existants".

La réplication s'arrêtera également si vous supprimez le rôle AWS Identity and Access Management (IAM), les autorisations AWS Key Management Service (AWS KMS) ou les autorisations liées à la politique de compartiment qui accordent à Amazon S3 les autorisations requises. Toutefois, nous ne recommandons pas ces approches, car elles entraînent l'échec de la réplication. Amazon S3 signale le statut de réplication pour les objets affectés sous la forme `FAILED`. Si les autorisations sont restaurées ultérieurement, les objets marqués `FAILED` ne sont pas automatiquement répliqués. Pour répliquer ces objets, vous devez utiliser la réplication par lot S3.

Réplication d'objets existants via la réplication par lot

La réplication par lot S3 diffère de la réplication en direct, qui réplique en continu et automatiquement les nouveaux objets entre les compartiments Amazon S3. Au lieu de cela, la réplication par lot S3 s'effectue à la demande sur des objets existants. La réplication par lot S3 vous permet de répliquer les types d'objets suivants :

- Objets qui existaient avant la mise en place d'une configuration de réplication
- Objets qui ont déjà été répliqués
- Objets dont la réplication a échoué

Vous pouvez répliquer ces objets à la demande à l'aide d'une tâche d'opérations par lot.

Pour commencer avec la réplication par lot, vous pouvez :

- Lancer la réplication par lot pour une nouvelle règle de réplication ou une nouvelle destination : vous pouvez créer une tâche de réplication par lot unique lors de la création de la première règle dans une nouvelle configuration de réplication ou de l'ajout d'un nouveau compartiment de destination à une configuration existante via la console Amazon S3.
- Lancer la réplication par lots pour une configuration de réplication existante : vous pouvez créer une nouvelle tâche de réplication par lots en utilisant S3 Batch Operations via la console Amazon S3, l' AWS Command Line Interface (AWS CLI) AWS SDKs, l'API REST ou Amazon S3.

Lorsque la tâche de réplication par lot est terminée, vous recevez un rapport de fin d'opérations. Pour plus d'informations sur la façon d'utiliser ce rapport pour examiner la tâche, consultez Suivi de l'état de la tâche et des rapports de fin de tâche.

Considérations sur la réplication par lot S3

Avant d'utiliser la réplication par lot S3, examinez la liste suivante de considérations :

- Votre compartiment source doit être associé à une configuration de réplication existante. Pour activer la réplication, consultez Présentation de la configuration de la réplication en direct et Exemples de configuration de la réplication en direct.
- Si le cycle de vie S3 est configuré pour votre compartiment, nous vous recommandons de désactiver vos règles de cycle de vie lorsque la tâche de réplication par lot est active. Cela permet d'assurer la parité entre les compartiments source et de destination. Sinon, ces compartiments peuvent diverger et le compartiment de destination ne sera pas un réplica exact du compartiment source. Par exemple, imaginez le scénario suivant:
  - Votre compartiment source possède plusieurs versions d'un objet et un marqueur de suppression sur cet objet.
  - Vos compartiments source et de destination disposent d'une configuration de cycle de vie pour retirer les marqueurs de suppression expirés.

  Dans ce scénario, la réplication par lot peut répliquer le marqueur de suppression dans le compartiment de destination avant de répliquer les versions de l'objet. Ce comportement peut avoir pour conséquence que votre configuration du cycle de vie marque le marqueur de suppression comme étant expiré et que le marqueur de suppression soit supprimé du compartiment de destination avant que les versions d'objet soient répliquées.

- Le rôle AWS Identity and Access Management (IAM) que vous spécifiez pour exécuter la tâche Batch Operations doit disposer des autorisations nécessaires pour effectuer l'opération de réplication par lots sous-jacente. Pour plus d'informations sur la création de rôles IAM, consultez Configuration d'un rôle IAM pour la réplication par lot S3.
- La réplication par lot nécessite un manifeste qui peut être généré par Amazon S3. Le manifeste généré doit être stocké dans le même emplacement Région AWS que le compartiment source. Si vous choisissez de ne pas générer le manifeste, vous pouvez fournir un rapport d'inventaire Amazon S3 ou un fichier CSV contenant les objets que vous souhaitez répliquer. Pour de plus amples informations, veuillez consulter the section called "Spécification d'un manifeste pour une tâche de réplication par lot".
- La réplication par lot ne prend pas en charge la réplication renouvelée d'objets qui ont été supprimés en spécifiant l'ID de version de l'objet dans le compartiment de destination. Pour répéter la réplication de ces objets, vous pouvez copier les objets sources en place avec une tâche de copie par lot. La copie de ces objets en place crée de nouvelles versions des objets dans le compartiment source et lance automatiquement la réplication vers le compartiment de destination. La suppression et la recréation du compartiment de destination ne déclenchent pas la réplication.

  Pour plus d'informations sur la copie par lot, consultez Exemples qui utilisent des opérations par lot pour copier des objets.
- Si vous utilisez une règle de réplication sur le compartiment source, veillez à mettre à jour votre configuration de réplication en accordant au rôle IAM attaché à la règle de réplication les autorisations appropriées pour répliquer des objets. Le rôle IAM doit disposer des autorisations nécessaires pour effectuer la réplication à la fois sur les compartiments source et de destination.
- Si vous soumettez plusieurs tâches de réplication par lot pour le même compartiment dans un court laps de temps, Amazon S3 exécute ces tâches simultanément.
- Si vous soumettez plusieurs tâches de réplication par lot pour deux compartiments différents, sachez qu'Amazon S3 risque de ne pas exécuter toutes les tâches simultanément. Si vous dépassez le nombre de tâches de réplication par lot pouvant être exécutées simultanément sur votre compte, Amazon S3 suspend les tâches les moins prioritaires pour travailler sur les tâches les plus prioritaires. Une fois les tâches les plus prioritaires terminées, toutes les tâches suspendues redeviennent actives.
- La réplication par lot n'est pas prise en charge pour les objets stockés dans les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.

- Pour répliquer par lot des objets S3 Intelligent-Tiering stockés dans les niveaux de stockage d'accès Archive ou Deep Archive, vous devez d'abord lancer une demande de restauration, puis attendre que les objets soient déplacés dans le niveau Accès fréquent.
- Une seule tâche de réplication par lots peut prendre en charge un manifeste contenant jusqu'à 20 milliards d'objets.

Spécification d'un manifeste pour une tâche de réplication par lot

Un manifeste est un objet Amazon S3 qui contient les clés d'objet sur lesquelles Amazon S3 doit agir. Pour créer une tâche de réplication par lot, vous devez fournir un manifeste généré par l'utilisateur ou demander à Amazon S3 de générer un manifeste basé sur votre configuration de réplication.

Si vous fournissez un manifeste généré par l'utilisateur, il doit se présenter sous la forme d'un rapport d'inventaire Amazon S3 ou d'un fichier CSV. Si les objets de votre manifeste se trouvent dans un compartiment versionné, vous devez spécifier la version IDs des objets. Seul l'objet dont l'ID de version est spécifié dans le manifeste sera répliqué. Pour en savoir plus sur la spécification d'un manifeste, consultez Spécification d'un manifeste.

Si vous choisissez de demander à Amazon S3 de générer un fichier manifeste en votre nom, les objets répertoriés utilisent le même compartiment source, le même préfixe et les mêmes balises que vos configurations de réplication sur le compartiment source. Avec un manifeste généré, Amazon S3 réplique toutes les versions éligibles de vos objets.

> **Note**
>
> Si vous choisissez qu'Amazon S3 génère le manifeste, celui-ci doit être stocké dans le même compartiment Région AWS que le compartiment source.

Filtres pour une tâche de réplication par lot

Lors de la création de votre tâche de réplication par lot, vous pouvez éventuellement spécifier des filtres supplémentaires, tels que la date de création d'objet et le statut de la réplication afin de réduire la portée de la tâche.

Vous pouvez filtrer les objets à répliquer sur la base de la valeur `ObjectReplicationStatuses`, en fournissant une ou plusieurs des valeurs suivantes :

- `"NONE"` – Indique qu'Amazon S3 n'a jamais tenté de répliquer l'objet auparavant.

- `"FAILED"` – Indique qu'Amazon S3 a déjà tenté mais n'a pas réussi à répliquer l'objet.
- `"COMPLETED"` – Indique qu'Amazon S3 a déjà répliqué l'objet avec succès.
- `"REPLICA"` – Indique que cet objet est un réplica répliqué par Amazon S3 à partir d'un autre compartiment source.

Pour plus d'informations sur les statuts de la réplication, consultez Obtention d'informations sur le statut de la réplication.

Si vous ne filtrez pas votre tâche de réplication par lot, les opérations par lot tentent de répliquer tous les objets (quel que soit leur `ObjectReplicationStatus`) dans votre manifeste qui répondent aux règles de votre configuration de réplication, à l'exception de certains objets qui ne sont pas répliqués par défaut. Pour de plus amples informations, consultez the section called "Qu'est-ce qui n'est pas répliqué avec les configurations de réplication ?".

En fonction de votre objectif, vous pouvez définir `ObjectReplicationStatuses` sur une ou plusieurs des valeurs suivantes :

- Pour répliquer uniquement des objets existants qui n'ont jamais été répliqués, incluez uniquement `"NONE"`.
- Pour réessayer de répliquer uniquement les objets qui n'ont pas pu être répliqués auparavant, incluez uniquement `"FAILED"`.
- Pour à la fois répliquer des objets existants et réessayer de répliquer des objets qui n'ont pas pu être répliqués auparavant, incluez `"NONE"` et `"FAILED"`.
- Pour remplir un compartiment de destination avec des objets répliqués vers une autre destination, incluez `"COMPLETED"`.
- Pour répliquer des objets qui ont déjà été répliqués, incluez `"REPLICA"`.

Rapport de fin de la réplication par lot

Lorsque vous créez une tâche de réplication par lot, vous pouvez demander un rapport de fin CSV. Ce rapport présente les objets, les codes de réussite ou d'échec de réplication, les résultats et les descriptions. Pour plus d'informations sur le suivi des tâches et les rapports de fin, consultez Rapports de fin de tâche.

Pour obtenir la liste des codes d'échec de réplication avec leurs descriptions, consultez Raisons de l'échec de la réplication Amazon S3.

Pour obtenir des informations sur la résolution des problèmes de réplication par lot, consultez Erreurs de réplication par lot.

Démarrer avec la réplication par lot

Pour en savoir plus sur l'utilisation de la réplication par lot, consultez Tutoriel : Réplication d'objets existants dans vos compartiments Amazon S3 avec la réplication par lot S3.

Configuration d'un rôle IAM pour la réplication par lot S3

Dans la mesure où la réplication par lot Amazon S3 est un type de tâche d'opérations par lot, vous devez créer un rôle AWS Identity and Access Management (IAM) pour accorder des autorisations d'opérations par lot afin d'effectuer des actions en votre nom. Vous devez également associer une politique IAM de réplication par lot au rôle IAM Opérations par lot.

Utilisez les procédures suivantes pour créer une politique et un rôle IAM qui donne aux opérations par lot l'autorisation de lancer une tâche de réplication par lot.

Pour créer une politique pour la réplication par lot

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Sous Access Management (Gestion des accès), choisissez Policies (politiques).
3. Choisissez Créer une politique.
4. Sur la page Spécifier les autorisations, choisissez JSON.
5. Insérez l'une des politiques suivantes, selon que votre manifeste est généré par Amazon S3 ou que vous fournissez votre propre manifeste. Pour de plus amples informations sur les manifestes, consultez Spécification d'un manifeste pour une tâche de réplication par lot.

   Avant d'utiliser ces politiques, remplacez les *`user input placeholders`* dans les politiques suivantes par les noms de vos compartiment source de réplication, compartiment de manifeste et compartiment de rapport d'achèvement.

   > **Note**
   >
   > Votre rôle IAM pour la réplication par lot nécessite des autorisations différentes, selon que vous générez un manifeste ou que vous en fournissez un. Assurez-vous donc de choisir la politique appropriée dans les exemples suivants.

Politique en cas d'utilisation et de stockage d'un manifeste généré par Amazon S3

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
      {
         "Action":[
            "s3:GetReplicationConfiguration",
            "s3:PutInventoryConfiguration"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket"
         ]
      },
      {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
```

```
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*",
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      }
   ]
}
```

Politique en cas d'utilisation d'un manifeste fourni par l'utilisateur

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Action":[
            "s3:InitiateReplication"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-source-bucket/*"
         ]
      },
            {
         "Action":[
            "s3:GetObject",
            "s3:GetObjectVersion"
         ],
         "Effect":"Allow",
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-manifest-bucket/*"
         ]
      },
      {
         "Effect":"Allow",
         "Action":[
            "s3:PutObject"
         ],
         "Resource":[
            "arn:aws:s3:::amzn-s3-demo-completion-report-bucket/*"
```

```
            ]
        }
    ]
}
```

6. Choisissez Suivant.
7. Spécifiez un nom pour la politique, puis choisissez Créer une politique.

Pour créer un rôle IAM pour la réplication par lot

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Sous Access Management (Gestion des accès), choisissez Roles (Rôles).
3. Choisissez Créer un rôle.
4. Choisissez Service AWS comme type d'entité de confiance. Dans la section Cas d'utilisation, choisissez S3 comme service et Opérations par lot S3 comme cas d'utilisation.
5. Choisissez Suivant. La page Ajouter des autorisations s'affiche. Dans la zone de recherche, recherchez la politique que vous avez créée dans la procédure précédente. Cochez la case à côté du nom de la politique, puis choisissez Suivant.
6. Sur la page Nommer, vérifier et créer, spécifiez un nom pour votre rôle IAM.
7. Dans la section Étape 1 : identités de confiance, vérifiez que votre rôle IAM utilise la politique d'approbation suivante :

   JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"batchoperations.s3.amazonaws.com"
         },
         "Action":"sts:AssumeRole"
      }
   ]
}
```

8. Dans la section Étape 2 : ajouter des autorisations, vérifiez que votre rôle IAM utilise la politique que vous avez créée précédemment.
9. Choisissez Créer un rôle.

Créer une tâche de réplication par lot pour de nouvelles destinations ou règles de réplication

Dans Amazon S3, la réplication en direct ne réplique aucun objet qui existait déjà dans votre compartiment source avant que vous ayez créé une configuration de réplication. La réplication en direct réplique automatiquement uniquement les objets nouveaux et mis à jour qui sont écrits dans le compartiment une fois la configuration de réplication créée. Pour répliquer des objets déjà existants, vous pouvez répliquer ces objets à la demande via la réplication par lot S3.

Lorsque vous créez la première règle dans une nouvelle configuration de réplication en direct ou que vous ajoutez un nouveau compartiment de destination à une configuration de réplication existante via la console Amazon S3, vous pouvez éventuellement créer une tâche de réplication par lot. Vous pouvez utiliser cette tâche de réplication par lot pour répliquer des objets existants dans le compartiment source vers le compartiment de destination.

Pour utiliser la réplication par lot pour une configuration existante sans ajouter un nouveau compartiment de destination, consultez Créer une tâche de réplication par lot pour les règles de réplication existantes.

Prérequis

Avant de créer votre tâche de réplication par lot, vous devez créer un rôle AWS Identity and Access Management (IAM) d'opérations par lot pour accorder à Amazon S3 les autorisations nécessaires pour effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Configuration d'un rôle IAM pour la réplication par lot S3.

Utilisation de la réplication par lot pour une nouvelle destination ou règle de réplication via la console Amazon S3

Lorsque vous créez la première règle dans une nouvelle configuration de réplication ou que vous ajoutez un nouveau compartiment de destination à une configuration existante via la console Amazon S3, vous pouvez choisir de créer une tâche de réplication par lot pour répliquer les objets existants dans le compartiment source.

Pour créer une tâche de réplication par lot lors de la création ou de la mise à jour d'une configuration de réplication

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments à usage général, choisissez le nom du compartiment qui contient les objets que vous souhaitez répliquer.
4. Pour créer une nouvelle règle de réplication ou modifier une règle existante, choisissez l'onglet Gestion et faites défiler l'écran jusqu'à Règles de réplication :

   - Pour créer une nouvelle règle de réplication, choisissez Créer une règle de réplication. Pour obtenir des exemples de configuration d'une règle de réplication de base, consultez Exemples de configuration de la réplication en direct.
   - Pour modifier une règle de réplication existante, sélectionnez la case d'option en regard du nom de la règle, puis choisissez Modifier la règle.
5. Créez votre nouvelle règle de réplication ou modifiez la destination de votre règle de réplication existante, puis choisissez Enregistrer.

   Une fois que vous avez créé la première règle dans une nouvelle configuration de réplication ou modifié une configuration existante pour ajouter une nouvelle destination, la boîte de dialogue Répliquer des objets existants ? s'affiche et vous permet de créer une tâche de réplication par lots.
6. Si vous souhaitez créer et exécuter cette tâche maintenant, choisissez Oui, répliquer les objets existants.

   Si vous souhaitez créer une tâche de réplication par lot ultérieurement, choisissez Non, ne pas répliquer les objets existants.
7. Si vous avez choisi Oui, répliquer les objets existants, la page Créer une tâche d'opérations par lots apparaît. La tâche de réplication par lot S3 comporte les paramètres suivants :

   Options d'exécution de tâche

   Si vous souhaitez que la tâche de réplication par lots S3 soit exécutée immédiatement, choisissez Exécuter automatiquement la tâche lorsqu'elle est prête. Si vous souhaitez exécuter la tâche ultérieurement, choisissez Attendre l'exécution de la tâche lorsqu'elle est prête.

> **Note**
>
> Si vous choisissez Exécuter automatiquement la tâche lorsqu'elle est prête, vous ne pourrez pas créer ni enregistrer un manifeste d'opérations par lot. Pour enregistrer le manifeste des opérations par lot, choisissez Attendre l'exécution de la tâche lorsqu'elle est prête.

Manifeste des opérations par lot

Si vous avez choisi Attendre l'exécution de la tâche lorsqu'elle est prête, la section Manifeste des opérations par lots apparaît. Le manifeste est la liste de tous les objets sur lesquels vous souhaitez exécuter l'action spécifiée. Vous pouvez choisir d'enregistrer le manifeste. Comme pour les fichiers Inventaire S3, le manifeste est enregistré en tant que fichier CSV et stocké dans un compartiment. Pour en savoir plus sur les manifestes des opérations par lot, consultez Spécification d'un manifeste.

Rapport de fin de tâche

Les opérations par lot S3 exécutent une seule tâche pour chaque objet spécifié dans le manifeste. Les rapports de fin de tâche fournissent un moyen facile de consulter les résultats de vos tâches dans un format consolidé sans nécessiter de configuration supplémentaire. Vous pouvez demander un rapport de fin pour toutes les tâches ou uniquement pour les tâches qui ont échoué. Pour en savoir plus sur les rapports de fin, consultez Rapports de fin de tâche.

Autorisations

L'une des causes les plus fréquentes des échecs de réplication est le manque d'autorisations dans le rôle fourni AWS Identity and Access Management (IAM). Pour plus d'informations sur la création de ce rôle, consultez Configuration d'un rôle IAM pour la réplication par lot S3. Veillez à créer ou à choisir un rôle IAM disposant des autorisations requises pour la réplication par lot.

8. Choisissez Enregistrer.

Créer une tâche de réplication par lot pour les règles de réplication existantes

Dans Amazon S3, la réplication en direct ne réplique aucun objet qui existait déjà dans votre compartiment source avant que vous ayez créé une configuration de réplication. La réplication en direct réplique automatiquement uniquement les objets nouveaux et mis à jour qui sont écrits dans le compartiment une fois la configuration de réplication créée. Pour répliquer des objets déjà existants, vous pouvez répliquer ces objets à la demande via la réplication par lot S3.

Vous pouvez configurer la réplication par lots S3 pour une configuration de réplication existante à l'aide de la console AWS SDKs, AWS Command Line Interface (AWS CLI) ou Amazon S3. Pour obtenir une vue d'ensemble de la réplication par lot, consultez Réplication d'objets existants via la réplication par lot.

Lorsque la tâche de réplication par lot est terminée, vous recevez un rapport de fin d'opérations. Pour plus d'informations sur l'utilisation du rapport pour examiner la tâche, consultez Suivi de l'état de la tâche et des rapports de fin de tâche.

Prérequis

Avant de créer votre tâche de réplication par lot, vous devez créer un rôle AWS Identity and Access Management (IAM) d'opérations par lot pour accorder à Amazon S3 les autorisations nécessaires pour effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Configuration d'un rôle IAM pour la réplication par lot S3.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Opérations par lot.
3. Choisissez Créer une tâche.
4. Vérifiez que la section Région AWS indique la région dans laquelle vous souhaitez créer votre tâche.
5. Dans la section Manifeste, spécifiez le format du manifeste que vous souhaitez utiliser. Le manifeste est la liste de tous les objets sur lesquels vous souhaitez exécuter l'action spécifiée. Pour en savoir plus sur les manifestes des opérations par lot, consultez Spécification d'un manifeste.

    - Si un manifeste a été préparé, choisissez S3 inventory report (manifest.json) (Rapport d'inventaire S3 (manifest.json)) ou CSV. Si votre manifeste se trouve dans un compartiment

versionné, vous pouvez spécifier l'ID de version du manifeste. Si vous ne spécifiez pas d'ID de version, les opérations par lot utilisent la version actuelle de votre manifeste. Pour plus d'informations sur la création d'un manifeste, consultez Spécification d'un manifeste.

> **Note**
>
> Si les objets de votre manifeste se trouvent dans un compartiment versionné, vous devez spécifier la version IDs des objets. Pour de plus amples informations, veuillez consulter Spécification d'un manifeste.

- Pour créer un manifeste basé sur votre configuration de la réplication, choisissez Create manifest using S3 Replication configuration (Créer un manifeste à l'aide de la configuration de réplication S3). Choisissez ensuite le compartiment source de votre configuration de la réplication.

6. (Facultatif) Si vous avez choisi Créer un manifeste à l'aide de la configuration de réplication S3, vous pouvez inclure des filtres supplémentaires, tels que la date de création de l'objet et le statut de réplication. Pour obtenir des exemples de filtrage par statut de réplication, consultez Spécification d'un manifeste pour une tâche de réplication par lot.
7. (Facultatif) Si vous avez choisi Créer un manifeste à l'aide de la configuration de réplication S3, vous pouvez enregistrer le manifeste généré. Pour enregistrer ce manifeste, sélectionnez Enregistrer le manifeste des opérations par lots. Spécifiez ensuite le compartiment de destination pour le manifeste et choisissez de chiffrer ou non le manifeste.

> **Note**
>
> Le manifeste généré doit être stocké dans le même emplacement Région AWS que le compartiment source.

8. Choisissez Suivant.
9. Sur la page Opérations, choisissez Répliquer, puis Suivant.
10. (Facultatif) Fournissez une description.
11. Ajustez la Priority (priorité) de la tâche si nécessaire. Un nombre plus élevé est synonyme de priorité supérieure. Simple Storage Service (Amazon S3) tente d'exécuter des tâches à priorité supérieure avant les tâches à priorité inférieure. Pour plus d'informations sur la priorité des tâches, consultez Affectation d'une priorité de tâche.

12. (Facultatif) Générez un rapport de fin de tâche. Pour générer ce rapport, sélectionnez Générer le rapport d'achèvement.

    Si vous choisissez de générer un rapport de fin de tâche, vous devez choisir de créer un rapport concernant Failed tasks only (uniquement les tâches ayant échoué) ou All tasks (toutes les tâches), et fournir un compartiment de destination pour le rapport.
13. Dans la section Autorisations, veillez à choisir un rôle IAM disposant des autorisations requises pour la réplication par lot. L'une des causes les plus courantes des échecs de réplication est l'insuffisance des autorisations dans le rôle IAM fourni. Pour plus d'informations sur la création de ce rôle, consultez Configuration d'un rôle IAM pour la réplication par lot S3.
14. (Facultatif) Ajoutez des identifications de tâche à la tâche de réplication par lot.
15. Choisissez Next (Suivant).
16. Passez en revue la configuration de la tâche, puis choisissez Créer une tâche.

Utilisation du AWS CLI avec un manifeste S3

L'exemple de commande `create-job` suivant crée une tâche de réplication par lot S3 à l'aide d'un manifeste généré par S3 pour le Compte AWS *`111122223333`*. Cet exemple réplique des objets existants et des objets qui n'ont pas pu être répliqués auparavant. Pour obtenir des informations sur le filtrage par statut de réplication, consultez Spécification d'un manifeste pour une tâche de réplication par lot.

Pour utiliser cette commande, remplacez *`user input placeholders`* par vos propres informations. Remplacez le rôle IAM `role/`*`batch-Replication-IAM-policy`* par le rôle IAM que vous avez créé précédemment. Pour de plus amples informations, veuillez consulter Configuration d'un rôle IAM pour la réplication par lot S3.

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest-generator '{"S3JobManifestGenerator": {"ExpectedBucketOwner":
 "111122223333", \
"SourceBucket": "arn:aws:s3:::amzn-s3-demo-source-bucket", \
"EnableManifestOutput": false, "Filter": {"EligibleForReplication": true, \
"ObjectReplicationStatuses": ["NONE","FAILED"]}}}' \
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
```

```
--no-confirmation-required \
--region source-bucket-region
```

> **Note**
>
> Vous devez lancer la tâche à partir du même compartiment Région AWS que celui de la source de réplication.

Une fois que vous avez lancé avec succès une tâche de réplication par lot, vous recevez l'ID de la tâche en tant que réponse. Vous pouvez surveiller cette tâche à l'aide de la commande `describe-job` suivante. Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

Utilisation du AWS CLI avec un manifeste fourni par l'utilisateur

L'exemple suivant crée une tâche de réplication par lot S3 à l'aide d'un manifeste défini par l'utilisateur pour le Compte AWS *111122223333*. Si les objets de votre manifeste se trouvent dans un compartiment versionné, vous devez spécifier la version IDs des objets. Seul l'objet dont l'ID de version est spécifié dans l'attaque de l'homme du milieu (HDM) sera répliqué. Pour plus d'informations sur la création d'un manifeste, consultez Spécification d'un manifeste.

Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations. Remplacez le rôle IAM `role/`*batch-Replication-IAM-policy* par le rôle IAM que vous avez créé précédemment. Pour de plus amples informations, veuillez consulter Configuration d'un rôle IAM pour la réplication par lot S3.

```
aws s3control create-job --account-id 111122223333 \
--operation '{"S3ReplicateObject":{}}' \
--report '{"Bucket":"arn:aws:s3:::amzn-s3-demo-completion-report-bucket",\
"Prefix":"batch-replication-report", \
"Format":"Report_CSV_20180820","Enabled":true,"ReportScope":"AllTasks"}' \
--manifest '{"Spec":{"Format":"S3BatchOperations_CSV_20180820",\
"Fields":["Bucket","Key","VersionId"]},\
"Location":{"ObjectArn":"arn:aws:s3:::amzn-s3-demo-manifest-bucket/manifest.csv",\
"ETag":"Manifest Etag"}}' \
```

```
--priority 1 \
--role-arn arn:aws:iam::111122223333:role/batch-Replication-IAM-policy \
--no-confirmation-required \
--region source-bucket-region
```

> **Note**
>
> Vous devez lancer la tâche à partir du même compartiment Région AWS que celui de la source de réplication.

Une fois que vous avez lancé avec succès une tâche de réplication par lot, vous recevez l'ID de la tâche en tant que réponse. Vous pouvez surveiller cette tâche à l'aide de la commande `describe-job` suivante.

```
aws s3control describe-job --account-id 111122223333 --job-id job-id --region source-bucket-region
```

Résolution des problèmes de réplication

Cette section contient des conseils de résolution des problèmes relatifs à la réplication Amazon S3 et des informations sur les erreurs de réplication par lot S3.

Rubriques

- Conseils pour la résolution des problèmes de réplication S3
- Erreurs de réplication par lot

Conseils pour la résolution des problèmes de réplication S3

Si les réplicas d'objets ne figurent pas dans le compartiment de destination après la configuration de la réplication, utilisez les conseils de dépannage suivants pour identifier les problèmes et les résoudre.

- La plupart des objets se répliquent en 15 minutes. Le temps nécessaire à Amazon S3 pour répliquer un objet dépend de plusieurs facteurs, y compris de la paire de régions source et de destination et de la taille de l'objet. Pour les objets volumineux, la réplication peut prendre plusieurs heures. Pour plus de visibilité sur les temps de réplication, vous pouvez utiliser le Contrôle du temps de réplication S3 (S3 RTC).

Si l'objet répliqué est volumineux, attendez un moment avant de vérifier s'il apparaît dans la destination. Vous pouvez également vérifier le statut de réplication de l'objet source. Si le statut de réplication de l'objet est `PENDING`, cela signifie qu'Amazon S3 n'a pas terminé la réplication. Si le statut de réplication de l'objet est `FAILED`, vérifiez la configuration de réplication définie sur le compartiment source.

En outre, pour recevoir des informations sur les échecs de réplication, vous pouvez configurer une réplication des notifications d'événements Amazon S3. Pour plus d'informations, consultez Recevoir des événements d'échec de réplication avec des notifications d'événements Amazon S3.

- Pour vérifier le statut de réplication d'un objet, vous pouvez appeler l'opération d'API `HeadObject`. L'opération d'API `HeadObject` renvoie le statut de réplication `PENDING`, `COMPLETED` ou `FAILED` d'un objet. En réponse à un appel d'API `HeadObject`, le statut de réplication est renvoyé dans l'en-tête `x-amz-replication-status`.

  > **Note**
  >
  > Pour exécuter `HeadObject`, vous devez disposer d'un accès en lecture sur l'objet que vous demandez. Une demande `HEAD` possède les mêmes options qu'une demande `GET`, sans effectuer d'opération `GET`. Par exemple, pour exécuter une `HeadObject` requête à l'aide de AWS Command Line Interface (AWS CLI), vous pouvez exécuter la commande suivante. Remplacez *`user input placeholders`* par vos propres informations.
  >
  > ```
  > aws s3api head-object --bucket amzn-s3-demo-source-bucket --key index.html
  > ```

- Si `HeadObject` renvoie les objets avec un statut de réplication `FAILED`, vous pouvez utiliser la réplication par lot S3 pour répliquer les objets ayant échoué. Pour de plus amples informations, veuillez consulter the section called "Réplication d'objets existants". Vous pouvez également charger à nouveau les objets ayant échoué dans le compartiment source, ce qui lancera la réplication des nouveaux objets.
- Dans la configuration de réplication du compartiment source, procédez aux vérifications suivantes :
  - L'Amazon Resource Name (ARN) du compartiment de destination est correct.
  - Le préfixe de nom de clé est correct. A titre d'exemple, si vous définissez la configuration pour répliquer des objets avec le préfixe `Tax`, seuls les objets dotés de noms de clés `Tax/document1` ou `Tax/document2` seront répliqués. Tout objet avec le nom de clé `document3` n'est pas répliqué.

  - Le statut de la règle de réplication est `Enabled`.
- Vérifiez que la gestion des versions n'a pas été suspendue sur aucun compartiment dans la configuration de la réplication. La gestion des versions doit être activée pour les compartiments source et de destination.
- Si une règle de réplication est définie pour Transférer la propriété de l'objet au propriétaire du compartiment de destination, le rôle AWS Identity and Access Management (IAM) utilisé pour la réplication doit disposer de cette `s3:ObjectOwnerOverrideToBucketOwner` autorisation. Cette autorisation est accordée sur la ressource (dans ce cas, le compartiment de destination). Par exemple, la déclaration `Resource` suivante montre comment accorder cette autorisation sur le compartiment de destination :

```
{
  "Effect":"Allow",
  "Action":[
    "s3:ObjectOwnerOverrideToBucketOwner"
  ],
  "Resource":"arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
}
```

- Si le compartiment de destination appartient à un autre compte, le propriétaire du compartiment de destination doit également accorder l'autorisation `s3:ObjectOwnerOverrideToBucketOwner` au propriétaire du compartiment source, conformément à la politique de compartiment de destination. Pour utiliser l'exemple de politique de compartiment suivant, remplacez *`user input placeholders`* par vos propres informations :

  JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1644945280205",
  "Statement": [
    {
      "Sid": "Stmt1644945277847",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
      },
      "Action": [
        "s3:ReplicateObject",
        "s3:ReplicateTags",
```

```
        "s3:ObjectOwnerOverrideToBucketOwner"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/*"
    }
  ]
}
```

> **Note**
>
> Si les paramètres de propriété de l'objet du compartiment de destination incluent Propriétaire du compartiment appliqué, vous n'avez pas besoin de mettre à jour le paramètre pour Remplacer la propriété de l'objet par le propriétaire du compartiment de destination dans la règle de réplication. Le changement de propriété de l'objet se produira par défaut. Pour plus d'informations sur la modification du propriétaire d'un réplica, consultez Modification du propriétaire d'un réplica.

- Si vous définissez la configuration de réplication dans un scénario entre comptes, dans lequel les compartiments source et de destination appartiennent à des propriétaires différents Comptes AWS, les compartiments de destination ne peuvent pas être configurés en tant que compartiment Requester Pays. Pour de plus amples informations, veuillez consulter Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation.
- Si les objets sources d'un compartiment sont chiffrés côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS), la règle de réplication doit être configurée pour inclure les objets chiffrés par AWS KMS. Assurez-vous de sélectionner Répliquer les objets chiffrés avec AWS KMS dans les paramètres de Chiffrement de la console Amazon S3. Sélectionnez ensuite une AWS KMS clé pour chiffrer les objets de destination.

> **Note**
>
> Si le compartiment de destination se trouve dans un autre compte, spécifiez une clé gérée par le AWS KMS client qui appartient au compte de destination. N'utilisez pas la clé par défaut gérée par Amazon S3 (`aws/s3`). L'utilisation de la clé par défaut chiffre les objets à l'aide de la clé gérée par Amazon S3 appartenant au compte source, empêchant ainsi le partage de l'objet avec un autre compte. Par conséquent, le compte de destination ne pourra pas accéder aux objets du compartiment de destination.

Pour utiliser une AWS KMS clé appartenant au compte de destination pour chiffrer les objets de destination, le compte de destination doit accorder les `kms:Encrypt` autorisations `kms:GenerateDataKey` et au rôle de réplication dans la politique de clé KMS. Pour utiliser l'exemple de déclaration suivant dans votre stratégie de clé KMS, remplacez *`user input placeholders`* par vos propres informations :

```
{
    "Sid": "AllowS3ReplicationSourceRoleToUseTheKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::123456789101:role/s3-replication-role"
    },
    "Action": ["kms:GenerateDataKey", "kms:Encrypt"],
    "Resource": "*"
}
```

Si vous utilisez un astérisque (`*`) pour la déclaration `Resource` dans la stratégie de clé AWS KMS , la stratégie autorise l'utilisation de la clé KMS uniquement pour le rôle de réplication. La stratégie n'autorise pas le rôle de réplication à augmenter ses autorisations.

Par défaut, la stratégie de clé KMS accorde à l'utilisateur root des autorisations complètes sur la clé. Ces autorisations peuvent être déléguées à d'autres utilisateurs du même compte. À moins que la stratégie de clé KMS source ne contienne des déclarations `Deny`, l'utilisation d'une politique IAM pour accorder des autorisations de rôle de réplication à la clé KMS source est suffisante.

> **Note**
>
> Les stratégies de clé KMS qui limitent l'accès à des plages d'adresses CIDR, à des points de terminaison de cloud privé virtuel (VPC) ou à des points d'accès S3 spécifiques peuvent entraîner l'échec de la réplication.

Si les clés KMS source ou de destination accordent des autorisations en fonction du contexte de chiffrement, vérifiez que les clés de compartiment Amazon S3 sont activées pour les compartiments. Si les clés de compartiment S3 sont activées dans les compartiments, le contexte de chiffrement doit être la ressource au niveau du compartiment, comme suit :

```
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-source-bucket"
     ]
"kms:EncryptionContext:arn:aws:arn": [
     "arn:aws:s3:::amzn-s3-demo-destination-bucket"
     ]
```

Outre les autorisations accordées par la stratégie de clé KMS, le compte source doit ajouter les autorisations minimales suivantes à la politique IAM du rôle de réplication :

```
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [
        "Source-KMS-Key-ARN"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "kms:GenerateDataKey",
        "kms:Encrypt"
    ],
    "Resource": [
        "Destination-KMS-Key-ARN"
    ]
}
```

Pour plus d'informations sur la réplication d'objets chiffrés avec AWS KMS, consultez la section Réplication d'objets chiffrés.

- Si le compartiment de destination appartient à un autre Compte AWS, vérifiez que le propriétaire du compartiment dispose d'une politique de compartiment sur le compartiment de destination qui autorise le propriétaire du compartiment source à répliquer des objets. Pour obtenir un exemple, consultez Configuration de la réplication pour des compartiments dans des comptes distincts.
- Pour utiliser Object Lock avec la réplication, vous devez accorder deux autorisations supplémentaires sur le compartiment S3 source dans le rôle AWS Identity and Access

Management (IAM) que vous utilisez pour configurer la réplication. Les deux autorisations supplémentaires sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d'une déclaration d'autorisation `s3:Get*`, cette déclaration répond à l'exigence. Pour de plus amples informations, veuillez consulter the section called "Utilisation du verrouillage d'objet avec la réplication S3".

- Si vos objets ne se répliquent toujours pas une fois que vous avez validé les autorisations, vérifiez la présence de déclarations `Deny` explicites dans les emplacements suivants :
  - Les déclarations `Deny` figurant dans les politiques du compartiment source ou de destination. La réplication échoue si la politique de compartiment refuse l'accès au rôle de réplication pour l'une des actions suivantes :

    Compartiment source :

    ```
            "s3:GetReplicationConfiguration",
            "s3:ListBucket",
            "s3:GetObjectVersionForReplication",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectVersionTagging"
    ```

    Compartiments de destination :

    ```
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
    ```

  - Les déclarations `Deny` ou les limites des autorisations associées au rôle IAM peuvent entraîner l'échec de la réplication.
  - `Deny`les instructions AWS Organizations contenues dans les politiques de contrôle des services (SCPs) associées aux comptes source ou de destination peuvent entraîner l'échec de la réplication.
  - `Deny`les instructions AWS Organizations contenues dans les politiques de contrôle des ressources (RCPs) associées aux compartiments source ou de destination peuvent entraîner l'échec de la réplication.
- Si un réplica d'objet ne figure pas dans le compartiment de destination, les problèmes suivants ont pu empêcher la réplication :
  - Amazon S3 ne réplique pas un objet figurant dans un compartiment source qui est lui-même un réplica créé par une autre configuration de réplication. Par exemple, si vous définissez

une configuration de réplication à partir du compartiment A vers le compartiment B vers le compartiment C, Amazon S3 ne réplique pas les réplicas d'objets dans le compartiment B vers le compartiment C.

- Le propriétaire d'un compartiment source peut accorder d'autres Comptes AWS autorisations pour télécharger des objets. Par défaut, le propriétaire du compartiment source ne possède aucune autorisation pour les objets créés par d'autres comptes. La configuration de réplication réplique uniquement les objets pour lesquels le propriétaire du compartiment source dispose des autorisations d'accès. Pour éviter ce problème, le propriétaire du compartiment source peut accorder d'autres Comptes AWS autorisations pour créer des objets de manière conditionnelle, en exigeant des autorisations d'accès explicites sur ces objets. Pour un exemple de politique, consultez Octroi d'autorisations intercomptes pour charger des objets tout en garantissant que le propriétaire du compartiment dispose d'un contrôle total.

- Supposons que vous ajoutiez une règle dans la configuration de réplication pour répliquer un sous-ensemble d'objets dotés d'une balise spécifique. Dans ce cas, vous devez attribuer une clé et une valeur de balise spécifiques au moment de la création de l'objet pour qu'Amazon S3 puisse répliquer l'objet. Si vous commencez par créer un objet, puis ajoutez la balise à l'objet existant, Amazon S3 ne réplique pas l'objet.
- Utilisez les notifications d'événements Amazon S3 pour vous avertir dans les cas où les objets ne sont pas répliqués vers leur Région AWS de destination. Les notifications d'événements Amazon S3 sont disponibles via Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) ou. AWS Lambda Pour de plus amples informations, veuillez consulter Recevoir des événements d'échec de réplication avec des notifications d'événements Amazon S3.

  Vous pouvez également consulter les raisons de l'échec de la réplication en utilisant les notifications d'événements Amazon S3. Pour consulter la liste des raisons d'échec, consultez Raisons de l'échec de la réplication Amazon S3.

Erreurs de réplication par lot

Pour résoudre les problèmes liés aux objets qui ne sont pas répliqués vers le compartiment de destination, vérifiez les différents types d'autorisations pour vos compartiments, le rôle de réplication et le rôle IAM utilisés pour créer la tâche de réplication par lot. Assurez-vous également de vérifier les paramètres de blocage de l'accès public et les paramètres de propriété d'objets S3 de vos compartiments.

Pour d'autres conseils de résolution des problèmes relatifs à l'utilisation des opérations par lot, consultez the section called "Résolution des problèmes d'opérations par lot".

Si vous avez configuré la réplication et que les objets ne se répliquent pas, consultez Pourquoi mes objets Amazon S3 ne se répliquent-ils pas lorsque je configure la réplication entre mes compartiments ? dans le AWS re:Post Knowledge Center.

Vous pouvez rencontrer l'une des erreurs suivantes avec la réplication par lot :

- La génération du manifeste n'a trouvé aucune clé correspondant aux critères du filtre.

  Cette erreur se produit pour l'une des raisons suivantes :

  - Quand des objets du compartiment source sont stockés dans la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

    Pour utiliser la réplication par lot sur ces objets, commencez par les restaurer dans la classe de stockage S3 Standard en utilisant une opération Restaurer (`S3InitiateRestoreObjectOperation`) dans une tâche d'opérations par lot. Pour plus d'informations, consultez Restauration d'un objet archivé et Restaurer des objets (opérations par lot). Une fois les objets restaurés, vous pouvez les répliquer à l'aide d'une tâche de réplication par lot.

  - Lorsque les critères de filtre fournis ne correspondent à aucun objet valide dans le compartiment source.

    Vérifiez et corrigez les critères de filtre. Par exemple, dans la règle de réplication par lot, le critère de filtre recherche tous les objets du compartiment source avec le préfixe `Tax/`. Si le nom du préfixe a été saisi de manière inexacte, avec une barre oblique au début et à la fin, `/Tax/`, plutôt qu'à la fin uniquement, aucun objet S3 n'a été trouvé. Pour résoudre l'erreur, corrigez le préfixe, dans ce cas, de `/Tax/` à `Tax/` dans la règle de réplication.

- L'opération par lot a un statut d'échec pour une raison : le rapport de tâche n'a pas pu être écrit dans votre compartiment de rapports.

  Cette erreur se produit si le rôle IAM utilisé pour la tâche d'opérations par lot ne parvient pas à placer le rapport de fin à l'emplacement spécifié lors de la création de la tâche. Pour résoudre cette erreur, vérifiez que le rôle IAM dispose de l'autorisation `s3:PutObject` pour le compartiment dans lequel vous souhaitez enregistrer le rapport de fin des opérations par lot. Nous vous recommandons de transmettre le rapport dans un compartiment autre que le compartiment source.

- L'opération par lot est terminée avec des échecs et le nombre total d'échecs n'est pas égal à 0.

Cette erreur se produit en cas de problèmes d'autorisations d'objet insuffisantes avec la tâche de réplication par lot en cours d'exécution. Si vous utilisez une règle de réplication pour votre tâche de réplication par lot, assurez-vous que le rôle IAM utilisé pour la réplication dispose des autorisations appropriées pour accéder aux objets depuis le compartiment source ou de destination. Vous pouvez également consulter le Rapport de fin de la réplication par lot pour connaître les raisons spécifiques de l'échec de la réplication Amazon S3.

- La tâche par lot s'est correctement exécutée, mais le nombre d'objets attendus dans le compartiment de destination n'est pas le même.

  Cette erreur se produit lorsqu'il existe une incompatibilité entre les objets répertoriés dans le manifeste fourni dans la tâche de réplication par lot et les filtres que vous avez sélectionnés lors de la création de la tâche. Vous pouvez également recevoir ce message lorsque les objets de votre compartiment source ne correspondent à aucune règle de réplication et ne sont pas inclus dans le manifeste généré.

Les échecs des opérations par lot se produisent après l'ajout d'une nouvelle règle de réplication à une configuration de réplication existante

Les opérations par lot tentent de répliquer des objets existants pour chaque règle de la configuration de réplication du compartiment source. En cas de problème avec l'une des règles de réplication existantes, des échecs peuvent survenir.

Le rapport de fin de la tâche d'opérations par lot explique les raisons de l'échec de la tâche. Pour obtenir une liste des erreurs courantes, consultez Raisons de l'échec de la réplication Amazon S3.

Surveillance de la réplication avec des métriques, des notifications d'événements et des statuts

Vous pouvez surveiller vos configurations de réplication en direct et vos tâches de réplication par lot S3 par le biais des mécanismes suivants :

- Métriques de réplication S3 : lorsque vous activez les métriques de réplication S3, Amazon CloudWatch émet des métriques que vous pouvez utiliser pour suivre les octets en attente, les opérations en attente et la latence de réplication au niveau des règles de réplication. Vous pouvez consulter les métriques de réplication S3 via les consoles Amazon S3 et Amazon CloudWatch . Dans la console Amazon S3, vous pouvez consulter ces métriques dans l'onglet Métriques du

compartiment source. Pour plus d'informations sur les métriques de réplication S3, consultez the section called "Utilisation des métriques de réplication S3".

- Métriques S3 Storage Lens : outre les métriques de réplication S3, vous pouvez utiliser les métriques de protection des données relatives à la réplication fournies par les tableaux de bord S3 Storage Lens. Par exemple, si vous utilisez les métriques gratuites de S3 Storage Lens, vous pouvez consulter des métriques telles que le nombre total d'octets répliqués depuis le compartiment source ou le nombre d'objets répliqués depuis le compartiment source.

  Pour auditer votre position de réplication globale, vous pouvez activer les métriques avancées dans S3 Storage Lens. Grâce aux métriques avancées de S3 Storage Lens, vous pouvez voir le nombre de règles de réplication de différents types dont vous disposez, y compris le nombre de règles de réplication dont la destination de réplication n'est pas valide.

  Pour plus d'informations sur l'utilisation des métriques de réplication dans S3 Storage Lens, consultez the section called "Affichage des métriques de réplication dans les tableaux de bord S3 Storage Lens".

- Notifications d'événements S3 — Les notifications d'événements S3 peuvent vous avertir au niveau de l'objet lorsque les objets ne se répliquent pas vers leur destination Région AWS ou lorsque les objets ne sont pas répliqués dans certains seuils. Les notifications d'événements S3 fournissent les types d'événements de réplication suivants : `s3:Replication:OperationFailedReplication`, `s3:Replication:OperationMissedThreshold`, `s3:Replication:OperationReplicatedAfterThreshold` et `s3:Replication:OperationNotTracked`.

  Les événements Amazon S3 sont disponibles via Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) ou. AWS Lambda Pour de plus amples informations, veuillez consulter the section called "Réception des événements d'échec de réplication".

- Valeurs de statut de réplication : vous pouvez également récupérer le statut de réplication de vos objets. Le statut de réplication peut vous aider à déterminer l'état actuel d'un objet en cours de réplication. Le statut de réplication d'un objet source renvoie soit `PENDING`, `COMPLETED` ou `FAILED`. Le statut de réplication d'un réplica renvoie `REPLICA`.

  Vous pouvez également utiliser les valeurs de statut de réplication lorsque vous créez des tâches de réplication par lot S3. Par exemple, vous pouvez utiliser ces valeurs de statut pour répliquer des objets qui n'ont jamais été répliqués ou dont la réplication a échoué.

Pour plus d'informations sur la récupération du statut de réplication de vos objets, consultez the section called "Obtention du statut de réplication". Pour plus d'informations sur l'utilisation de ces valeurs avec la réplication par lot, consultez the section called "Filtres pour une tâche de réplication par lot".

Rubriques

- Utilisation des métriques de réplication S3
- Affichage des métriques de réplication dans les tableaux de bord S3 Storage Lens
- Recevoir des événements d'échec de réplication avec des notifications d'événements Amazon S3
- Obtention d'informations sur le statut de la réplication

Utilisation des métriques de réplication S3

Les métriques de réplication S3 fournissent des métriques détaillées pour les règles de réplication dans votre configuration de réplication. Grâce aux métriques de réplication, vous pouvez suivre la minute-by-minute progression en suivant les octets en attente, les opérations en attente, les opérations dont la réplication a échoué et la latence de réplication.

> **Note**
>
> - Les métriques de réplication S3 sont facturées au même tarif que les métriques CloudWatch personnalisées d'Amazon. Pour plus d'informations, consultez les CloudWatchtarifs Amazon.
> - Si vous utilisez S3 Replication Time Control, Amazon CloudWatch commence à communiquer les métriques de réplication 15 minutes après avoir activé S3 RTC sur la règle de réplication correspondante.

Les métriques de réplication S3 sont activées automatiquement lorsque vous activez le contrôle du temps de réplication S3 (S3 RTC). Vous pouvez également activer les métriques de réplication S3 indépendamment du contrôle du temps de réplication S3 lors de la création ou de la modification d'une règle. S3 RTC inclut d'autres fonctions telles qu'un contrat de niveau de service (SLA) et des notifications pour les seuils non respectés. Pour de plus amples informations, veuillez consulter Satisfaction aux exigences de conformité à l'aide du contrôle du temps de réplication S3.

Lorsque les métriques de réplication S3 sont activées, Amazon S3 publie les métriques suivantes sur Amazon CloudWatch. CloudWatchles indicateurs sont fournis dans la mesure du possible.

Nom de la métrique	Description de la métrique	À quels objets cette métrique s'applique-t-elle ?	Dans quelle région cette métrique est-elle publiée ?	Cette métrique est-elle toujours publiée si le compartiment de destination est supprimé ?	Cette métrique est-elle toujours publiée si la réplication n'a pas lieu ?
Octets en attente de réplication	Nombre total d'octets d'objets en attente de réplication pour une règle de réplication donnée.	Cette métrique s'applique uniquement aux nouveaux objets répliqués avec la réplication interrégionale S3 (S3 CRR) ou la réplication S3 sur une même région (S3 SRR).	Cette métrique est publiée dans la région du compartiment de destination.	Non	Oui
Latence de réplication	Nombre maximal de secondes pendant lesquelles le compartiment de	Cette métrique s'applique uniquement aux nouveaux objets	Cette métrique est publiée dans la région du compartiment de destination.	Non	Oui

Nom de la métrique	Description de la métrique	À quels objets cette métrique s'applique-t-elle ?	Dans quelle région cette métrique est-elle publiée ?	Cette métrique est-elle toujours publiée si le compartiment de destination est supprimé ?	Cette métrique est-elle toujours publiée si la réplication n'a pas lieu ?
	destination de réplication se trouve derrière le compartiment source pour une règle de réplication donnée.	répliqués avec S3 CRR ou S3 SRR.			

Nom de la métrique	Description de la métrique	À quels objets cette métrique s'applique-t-elle ?	Dans quelle région cette métrique est-elle publiée ?	Cette métrique est-elle toujours publiée si le compartiment de destination est supprimé ?	Cette métrique est-elle toujours publiée si la réplication n'a pas lieu ?
Opérations en attente de réplication	Nombre d'opérations en attente de réplication pour une règle de réplication donnée. Cette métrique suit les opérations liées aux objets, aux marqueurs de suppression, aux balises, aux listes de contrôle d'accès (ACLs) et au verrouillage des objets S3.	Cette métrique s'applique uniquement aux nouveaux objets répliqués avec S3 CRR ou S3 SRR.	Cette métrique est publiée dans la région du compartiment de destination.	Non	Oui

Nom de la métrique	Description de la métrique	À quels objets cette métrique s'applique-t-elle ?	Dans quelle région cette métrique est-elle publiée ?	Cette métrique est-elle toujours publiée si le compartiment de destination est supprimé ?	Cette métrique est-elle toujours publiée si la réplication n'a pas lieu ?
Échec de la réplication des opérations	Nombre d'opérations pour lesquelles la réplication a échoué pour une règle de réplication donnée. Cette métrique suit les opérations liées aux objets, aux marqueurs de suppression, aux balises, aux listes de contrôle d'accès (ACLs) et au verrouillage d'objets. Échec de la réplication des opérations suit les	Cette métrique s'applique aux nouveaux objets répliqués avec S3 CRR ou S3 SRR, ainsi qu'aux objets existants répliqués avec la réplication par lot S3. **Note** Si une tâche de réplication par lots S3 ne	Cette métrique est publiée dans la région du compartiment source.	Oui	Non

Nom de la métrique	Description de la métrique	À quels objets cette métrique s'applique-t-elle ?	Dans quelle région cette métrique est-elle publiée ?	Cette métrique est-elle toujours publiée si le compartiment de destination est supprimé ?	Cette métrique est-elle toujours publiée si la réplication n'a pas lieu ?
	échecs de réplication S3 agrégés par minute. Pour identifier les objets spécifiques pour lesquels la réplication a échoué et les raisons de leur échec, abonnez-vous à l'événement `OperationFailedReplication` dans les notifications d'événements Amazon S3. Pour de plus amples informations, veuillez consulter	s'exécute pas du tout, les métriques ne sont pas envoyées à Amazon CloudWatch. Par exemple, votre tâche ne sera pas exécutée si vous ne disposez pas des autorisat			

Nom de la métrique	Description de la métrique	À quels objets cette métrique s'applique-t-elle ?	Dans quelle région cette métrique est-elle publiée ?	Cette métrique est-elle toujours publiée si le compartiment de destination est supprimé ?	Cette métrique est-elle toujours publiée si la réplication n'a pas lieu ?
	Recevoir des événements d'échec de réplication avec des notifications d'événements Amazon S3.	ions nécessaires pour exécuter une tâche de réplication par lot S3, ou si les balises ou le préfixe de votre configuration de réplication ne correspondent pas.			

Pour plus d'informations sur l'utilisation de ces métriques dans CloudWatch, consultezthe section called “Métriques de réplication S3 dans CloudWatch”.

Activation des métriques de réplication S3

Vous pouvez commencer à utiliser des métriques de réplication S3 avec une règle de réplication nouvelle ou existante. Pour obtenir des instructions complètes sur la création de règles de réplication, consultez Configuration d'une réplication pour des compartiments dans le même compte. Vous pouvez choisir d'appliquer votre règle de réplication à un compartiment S3 entier ou à des objets Amazon S3 avec un préfixe ou une balise spécifique.

Cette rubrique fournit des instructions pour activer les métriques de réplication S3 dans votre configuration de réplication lorsque les compartiments source et de destination sont détenus par des Comptes AWS identiques ou différents.

Pour activer les métriques de réplication à l'aide de AWS Command Line Interface (AWS CLI), vous devez ajouter une configuration de réplication au compartiment source en `Metrics` activant. Dans cet exemple de configuration, les objets sous le préfixe *`Tax`* sont répliqués dans le compartiment de destination *`amzn-s3-demo-bucket`* et des métriques sont générées pour ces objets.

```
{
    "Rules": [
        {
            "Status": "Enabled",
            "Filter": {
                "Prefix": "Tax"
            },
            "Destination": {
                "Bucket": "arn:aws:s3:::amzn-s3-demo-bucket",
                "Metrics": {
                    "Status": "Enabled"
                }
            },
            "Priority": 1
        }
    ],
    "Role": "IAM-Role-ARN"
}
```

Affichage des métriques de réplication

Vous pouvez consulter les métriques de réplication S3 dans l'onglet Metrics du bucket source à usage général de la console Amazon S3. Ces CloudWatch statistiques Amazon sont également disponibles dans la CloudWatch console Amazon. Lorsque vous activez les métriques de réplication S3, Amazon CloudWatch émet des métriques que vous pouvez utiliser pour suivre les octets en attente, les opérations en attente et la latence de réplication au niveau des règles de réplication.

Les métriques de réplication S3 sont activées automatiquement lorsque vous activez la réplication avec le contrôle du temps de réplication S3 (S3 RTC) à l'aide de la console Amazon S3 ou de l'API REST Amazon S3. Vous pouvez également activer les métriques de réplication S3 indépendamment du contrôle du temps de réplication S3 lors de la création ou de la modification d'une règle.

Si vous utilisez S3 Replication Time Control, Amazon CloudWatch commence à communiquer les métriques de réplication 15 minutes après avoir activé S3 RTC sur la règle de réplication correspondante. Pour de plus amples informations, veuillez consulter Utilisation des métriques de réplication S3.

Les métriques de réplication suivent la règle IDs de configuration de la réplication. Un ID de règle de réplication peut être spécifique à un préfixe, à une balise ou à une combinaison des deux.

Pour plus d'informations sur CloudWatch les métriques pour Amazon S3, consultezSurveillance des métriques avec Amazon CloudWatch.

Prérequis

Créez une règle de réplication avec les métriques de réplication S3 activées. Pour de plus amples informations, veuillez consulter the section called "Activation des métriques de réplication".

Pour afficher les métriques de réplication S3 via l'onglet Métriques du compartiment source

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment source qui contient les objets pour lesquels vous souhaitez obtenir des métriques de réplication.
4. Sélectionnez l'onglet Métriques.
5. Sous Métriques de réplication, choisissez les règles de réplication pour lesquelles vous souhaitez consulter les métriques.

6. Choisissez Display charts (Afficher les graphiques).

   Amazon S3 affiche les graphiques Latence de réplication, Octets en attente de réplication, Opérations en attente de réplication et Échec de la réplication des opérations pour les règles que vous avez sélectionnées.

Affichage des métriques de réplication dans les tableaux de bord S3 Storage Lens

Outre les métriques de réplication S3, vous pouvez utiliser les métriques de protection des données relatives à la réplication fournies par S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Pour plus d'informations, consultez Utilisation de S3 Storage Lens pour protéger vos données.

S3 Storage Lens fournit deux niveaux de métriques : les métriques gratuites et des métriques et recommandations avancées, que vous pouvez utiliser moyennant des frais supplémentaires. Les métriques et recommandations avancées vous donnent accès à des métriques et à des fonctionnalités supplémentaires pour mieux comprendre votre stockage. Pour obtenir des informations sur la tarification de S3 Storage Lens, consultez la tarification Amazon S3.

Si vous utilisez les métriques gratuites de S3 Storage Lens, vous pouvez consulter des métriques telles que le nombre total d'octets répliqués depuis le compartiment source ou le nombre d'objets répliqués depuis le compartiment source.

Pour auditer votre position de réplication globale, vous pouvez activer les métriques avancées dans S3 Storage Lens. Grâce aux métriques avancées de S3 Storage Lens, vous pouvez voir le nombre de règles de réplication de différents types dont vous disposez, y compris le nombre de règles de réplication dont la destination de réplication n'est pas valide.

Pour obtenir la liste complète des métriques S3 Storage Lens, y compris les métriques de réplication figurant dans chaque niveau, consultez Glossaire des métriques S3 Storage Lens.

Prérequis

Créez une configuration de réplication en direct ou une tâche de réplication par lot S3.

Pour afficher les métriques de réplication dans Amazon S3 Storage Lens

1. Créez un tableau de bord S3 Storage Lens. Pour step-by-step obtenir des instructions, voirthe section called "Utilisation de la console S3".

2. (Facultatif) Lors de la configuration de votre tableau de bord, si vous souhaitez voir toutes les métriques de réplication de S3 Storage Lens, sélectionnez Métriques et recommandations avancées, puis sélectionnez Métriques avancées sur la protection des données. Pour obtenir la liste complète des métriques, consultez Glossaire des métriques S3 Storage Lens.

   Si vous activez les métriques et recommandations avancées, vous pouvez obtenir des informations exploitables supplémentaires sur vos configurations de réplication. Par exemple, vous pouvez utiliser les métriques de décompte des règles de réplication S3 Storage Lens pour obtenir des informations détaillées sur vos compartiments configurés pour la réplication. Ces informations incluent les règles de réplication au sein des compartiments et des régions et entre eux. Pour de plus amples informations, veuillez consulter the section called "Décompte du nombre total de règles de réplication pour chaque compartiment".
3. Après avoir créé votre tableau de bord, ouvrez-le et choisissez l'onglet Compartiments.
4. Faites défiler jusqu'à la section Buckets (Compartiments). Sous Metrics categories (Catégories de métriques), choisissez Data protection (Protection des données). Effacez ensuite Summary (Résumé).
5. Pour filtrer la liste Compartiments afin d'afficher uniquement les métriques de réplication, choisissez l'icône des préférences ( ).
6. Désactivez les boutons bascules pour toutes les métriques sur la protection des données jusqu'à ce que seules les métriques de réplication restent sélectionnées.
7. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.
8. Choisissez Continuer.

Recevoir des événements d'échec de réplication avec des notifications d'événements Amazon S3

Si vous avez activé les métriques de réplication S3 sur votre configuration de réplication, vous pouvez configurer les notifications d'événements Amazon S3 pour vous avertir lorsque les objets ne sont pas répliqués vers leur Région AWS de destination. Si vous avez activé le contrôle du temps de réplication S3 (S3 RTC) dans votre configuration de réplication, vous pouvez également être averti lorsque les objets ne sont pas répliqués dans le délai maximal de 15 minutes fixé par S3 RTC pour la réplication.

En utilisant les types d'`Replication`événements suivants, vous pouvez surveiller la minute-by-minute progression des événements de réplication en suivant les octets en attente, les opérations en attente et la latence de réplication. Pour plus d'informations sur les métriques de réplication S3, consultez Utilisation des métriques de réplication S3.

- Le type d'événement `s3:Replication:OperationFailedReplication` vous avertit lorsqu'un objet éligible à la réplication n'a pas pu être répliqué.
- Le type d'événement `s3:Replication:OperationMissedThreshold` vous avertit lorsqu'un objet éligible à la réplication et qui utilise S3 RTC dépasse le délai maximal de 15 minutes pour la réplication.
- Le type d'événement `s3:Replication:OperationReplicatedAfterThreshold` vous avertit lorsqu'un objet éligible à la réplication et qui utilise S3 RTC est répliqué après le délai maximal de 15 minutes.
- Le type d'événement `s3:Replication:OperationNotTracked` vous avertit lorsqu'un objet éligible à la réplication en direct (réplication sur une même région [SRR] ou réplication interrégionale [CRR]) n'est plus suivi par les métriques de réplication.

Pour obtenir des descriptions complètes de tous les types d'événements de réplication pris en charge, consultez the section called "Types d'événements pris en charge pour SQS, SNS et Lambda".

Pour obtenir la liste des codes d'échec capturés par les notifications d'événements S3, consultez Raisons de l'échec de la réplication Amazon S3.

Vous pouvez recevoir des notifications d'événements S3 via Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) ou AWS Lambda. Pour de plus amples informations, veuillez consulter the section called "Notifications d'événements Amazon S3".

Pour obtenir des instructions sur la configuration des notifications d'événements Amazon S3, consultez Activation des notifications d'événements.

> **Note**
>
> Outre l'activation des notifications d'événements, veillez également à activer les métriques de réplication S3. Pour de plus amples informations, veuillez consulter the section called "Activation des métriques de réplication".

Le message suivant est un exemple de message envoyé par Amazon S3 pour publier un événement `s3:Replication:OperationFailedReplication`. Pour de plus amples informations, veuillez consulter the section called "Structure des messages d'événements".


```
{
  "Records": [
    {
      "eventVersion": "2.2",
      "eventSource": "aws:s3",
      "awsRegion": "us-east-1",
      "eventTime": "2024-09-05T21:04:32.527Z",
      "eventName": "Replication:OperationFailedReplication",
      "userIdentity": {
        "principalId": "s3.amazonaws.com"
      },
      "requestParameters": {
        "sourceIPAddress": "s3.amazonaws.com"
      },
      "responseElements": {
        "x-amz-request-id": "123bf045-2b4b-4ca8-a211-c34a63c59426",
        "x-amz-id-2":
 "12VAWNDIHnwJsRhTccqQTeAPoXQmRt22KkewMV8G3XZihAuf9CLDdmkApgZzudaIe2KlLfDqGS0="
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "ReplicationEventName",
        "bucket": {
          "name": "amzn-s3-demo-bucket1",
          "ownerIdentity": {
            "principalId": "111122223333"
          },
          "arn": "arn:aws:s3:::amzn-s3-demo-bucket1"
        },
        "object": {
          "key": "replication-object-put-test.png",
          "size": 520080,
          "eTag": "e12345ca7e88a38428305d3ff7fcb99f",
          "versionId": "abcdeH0Xp66ep__QDjR76LK7Gc9X4wKO",
          "sequencer": "0066DA1CBF104C0D51"
        }
      },
      "replicationEventData": {
        "replicationRuleId": "notification-test-replication-rule",
```

```
        "destinationBucket": "arn:aws:s3:::amzn-s3-demo-bucket2",
        "s3Operation": "OBJECT_PUT",
        "requestTime": "2024-09-05T21:03:59.168Z",
        "failureReason": "AssumeRoleNotPermitted"
      }
    }
  ]
}
```

Raisons de l'échec de la réplication Amazon S3

Le tableau suivant répertorie les raisons des échecs de la réplication Amazon S3. Vous pouvez consulter ces raisons en recevant l'événement `s3:Replication:OperationFailedReplication` avec les notifications d'événements Amazon S3, puis en examinant la valeur `failureReason`.

Vous pouvez également consulter ces raisons d'échec dans un rapport de fin de la réplication par lot S3. Pour plus d'informations, consultez Rapport de fin de la réplication par lot.

Raison de l'échec de la réplication	Description
`AssumeRoleNotPermitted`	Amazon S3 ne peut pas assumer le rôle AWS Identity and Access Management (IAM) spécifié dans la configuration de réplication ou dans le job Batch Operations.
`DstBucketInvalidRegion`	Le compartiment de destination ne se trouve pas dans le même compartiment Région AWS que celui spécifié par le job Batch Operations. Cette erreur est spécifique à la réplication par lot.
`DstBucketNotFound`	Amazon S3 n'est pas en mesure de trouver le compartiment de destination spécifié dans la configuration de la réplication.
`DstBucketObjectLockConfigMissing`	Pour répliquer des objets à partir d'un compartiment source avec le verrouillage d'objets activé, il doit également être activé dans le compartiment de destination. Cette

Raison de l'échec de la réplication	Description
	erreur indique que le verrouillage d'objets n'est peut-être pas activé dans le compartiment de destination. Pour plus d'informations, consultez Considérations relatives au verrouillage d'objet.
`DstBucketUnversioned`	La gestion des versions n'est pas activée pour le compartiment de destination S3. Pour répliquer des objets avec la réplication S3, activez la gestion des versions pour le compartiment de destination.
`DstDelObjNotPermitted`	Amazon S3 n'est pas en mesure de répliquer des marqueurs de suppression vers le compartiment de destination. L'autorisation `s3:ReplicateDelete` peut être manquante pour le compartiment de destination.
`DstKmsKeyInvalidState`	L'état de la clé AWS Key Management Service (AWS KMS) du compartiment de destination n'est pas valide. Vérifiez et activez la AWS KMS clé requise. Pour plus d'informations sur la gestion des AWS KMS clés, consultez la section État des AWS KMS clés dans le manuel du AWS Key Management Service développeur.
`DstKmsKeyNotFound`	La AWS KMS clé configurée pour le compartiment de destination dans la configuration de réplication n'existe pas.

Raison de l'échec de la réplication	Description
`DstMultipartCompleteNotPermitted`	Amazon S3 n'est pas en mesure de terminer les chargements partitionnés des objets dans le compartiment de destination. L'autorisation `s3:ReplicateObject` peut être manquante pour le compartiment de destination.
`DstMultipartInitNotPermitted`	Amazon S3 n'est pas en mesure de lancer les chargements partitionnés des objets dans le compartiment de destination. L'autorisation `s3:ReplicateObject` peut être manquante pour le compartiment de destination.
`DstMultipartUploadNotPermitted`	Amazon S3 n'est pas en mesure de charger les objets de chargement partitionné dans le compartiment de destination. L'autorisation `s3:ReplicateObject` peut être manquante pour le compartiment de destination.
`DstObjectHardDeleted`	La réplication par lot S3 ne prend pas en charge la réplication répétée d'objets supprimés avec l'ID de version de l'objet dans le compartiment de destination. Cette erreur est spécifique à la réplication par lot.
`DstPutAclNotPermitted`	Amazon S3 n'est pas en mesure de répliquer les listes de contrôle d'accès aux objets (ACLs) dans le compartiment de destination. L'autorisation `s3:ReplicateObject` peut être manquante pour le compartiment de destination.

Raison de l'échec de la réplication	Description
`DstPutLegalHoldNotPermitted`	Amazon S3 n'est pas en mesure de bloquer légalement les objets de destination lorsqu'il réplique des objets immuables. L'autorisation `s3:PutObjectLegalHold` peut être manquante pour le compartiment de destination. Pour plus d'informations, consultez Conservations légales.
`DstPutObjectNotPermitted`	Amazon S3 n'est pas en mesure de répliquer des objets vers le compartiment de destination. Cela peut se produire lorsque les autorisations requises (`s3:ReplicateObject` ou `s3:ObjectOwnerOverrideToBucketOwner` autorisations) sont manquantes pour le compartiment de destination ou lorsque la politique AWS KMS clé n'autorise pas le rôle de réplication du compartiment source à utiliser la AWS KMS clé (`kms:Decrypt` et `kms:GenerateDataKey*` les actions) dans le compartiment de destination.
`DstPutRetentionNotPermitted`	Amazon S3 n'est pas en mesure d'attribuer une période de rétention aux objets de destination lorsqu'il réplique des objets immuables. L'autorisation `s3:PutObjectRetention` peut être manquante pour le compartiment de destination.
`DstPutTaggingNotPermitted`	Amazon S3 n'est pas en mesure de répliquer des balises d'objets vers le compartiment de destination. L'autorisation `s3:ReplicateObject` peut être manquante pour le compartiment de destination.

Raison de l'échec de la réplication	Description
`DstVersionNotFound`	Amazon S3 n'est pas en mesure de trouver la version d'objet requise dans le compartiment de destination pour lequel les métadonnées doivent être répliquées.
`InitiateReplicationNotPermitted`	Amazon S3 n'est pas en mesure de lancer la réplication sur des objets. L'autorisation `s3:InitiateReplication` peut être manquante pour la tâche d'opérations par lot. Cette erreur est spécifique à la réplication par lot.
`SrcBucketInvalidRegion`	Le compartiment source ne se trouve pas dans le même compartiment Région AWS que celui spécifié par le job Batch Operations. Cette erreur est spécifique à la réplication par lot.
`SrcBucketNotFound`	Amazon S3 n'est pas en mesure de trouver le compartiment source.
`SrcBucketReplicationConfigMissing`	Amazon S3 n'a pas trouvé de configuration de réplication pour le compartiment source.

Raison de l'échec de la réplication	Description
`SrcGetAclNotPermitted`	Amazon S3 n'est pas en mesure d'accéder à l'objet dans le compartiment source pour la réplication. L'autorisation `s3:GetObjectVersionAcl` peut être manquante pour l'objet du compartiment source. Les objets du compartiment source doivent appartenir au propriétaire du compartiment. Si ACLs elles sont activées, vérifiez si la propriété de l'objet est définie sur Bucket owner preferred ou Object Writer. Si la propriété de l'objet est définie sur Propriétaire du compartiment préféré, les objets du compartiment source doivent disposer de la liste ACL `bucket-owner-full-control` pour que le propriétaire du compartiment devienne propriétaire de l'objet. Le compte source peut s'approprier tous les objets de son compartiment en définissant Object Ownership sur Bucket owner (appliqué et en désactivant ACLs).
`SrcGetLegalHoldNotPermitted`	Amazon S3 n'est pas en mesure d'accéder aux informations de conservation légale du verrouillage d'objet S3.
`SrcGetObjectNotPermitted`	Amazon S3 n'est pas en mesure d'accéder à l'objet dans le compartiment source pour la réplication. L'autorisation `s3:GetObjectVersionForReplication` peut être manquante pour le compartiment source.
`SrcGetRetentionNotPermitted`	Amazon S3 n'est pas en mesure d'accéder aux informations de période de conservation du verrouillage des objets S3.

Raison de l'échec de la réplication	Description
`SrcGetTaggingNotPermitted`	Amazon S3 n'est pas en mesure d'accéder aux informations de la balise d'objet depuis le compartiment source. L'autorisation `s3:GetObjectVersionTagging` peut être manquante pour le compartiment source.
`SrcHeadObjectNotPermitted`	Amazon S3 n'est pas en mesure de récupérer les métadonnées de l'objet depuis le compartiment source. L'autorisation `s3:GetObjectVersionForReplication` peut être manquante pour le compartiment source.
`SrcKeyNotFound`	Amazon S3 n'est pas en mesure de trouver la clé de l'objet source à répliquer. L'objet source a peut-être été supprimé avant la fin de la réplication.
`SrcKmsKeyInvalidState`	L'état de la AWS KMS clé du compartiment source n'est pas valide. Vérifiez et activez la AWS KMS clé requise. Pour plus d'informations sur la gestion des AWS KMS clés, consultez la section État des AWS KMS clés dans le manuel du AWS Key Management Service développeur.
`SrcObjectNotEligible`	Certains objets ne sont pas éligibles à la réplication. Cela peut être dû à la classe de stockage de l'objet ou aux balises de l'objet qui ne correspondent pas à la configuration de réplication.
`SrcObjectNotFound`	L'objet source n'existe pas.
`SrcReplicationNotPending`	Amazon S3 a déjà répliqué cet objet. Cet objet n'est plus en attente de réplication.

Raison de l'échec de la réplication	Description
`SrcVersionNotFound`	Amazon S3 n'est pas en mesure de trouver la version de l'objet source à répliquer. La version de l'objet source a peut-être été supprimée avant la fin de la réplication.

Rubriques en relation

Configuration des autorisations pour la réplication en direct

Résolution des problèmes de réplication

Obtention d'informations sur le statut de la réplication

Le statut de réplication peut vous aider à déterminer l'état actuel d'un objet répliqué. Le statut de réplication d'un objet source renvoie soit `PENDING`, `COMPLETED` ou `FAILED`. Le statut de réplication d'un réplica renvoie `REPLICA`.

Vous pouvez également utiliser les valeurs de statut de réplication lorsque vous créez des tâches de réplication par lot S3. Par exemple, vous pouvez utiliser ces valeurs de statut pour répliquer des objets qui n'ont jamais été répliqués ou dont la réplication a échoué. Pour plus d'informations sur l'utilisation de ces valeurs avec la réplication par lot, consultez the section called "Utilisation des informations de statut de réplication avec les tâches de réplication par lot".

Rubriques

- Vue d'ensemble des statuts de réplication
- Statut de la réplication en cas de réplication vers plusieurs compartiments de destination
- Statut de la réplication si la synchronisation des modifications de réplica Simple Storage Service (Amazon S3) est activée
- Utilisation des informations de statut de réplication avec les tâches de réplication par lot
- Recherche du statut de réplication

Vue d'ensemble des statuts de réplication

Dans le cadre de la réplication, vous disposez d'un compartiment source dans lequel vous configurez la réplication et d'un ou de plusieurs compartiments de destination dans lesquels Amazon S3 réplique

les objets. Lorsque vous demandez un objet (à l'aide de `GetObject`) ou des métadonnées d'objet (à l'aide de `HeadObject`) à partir de ces compartiments, Amazon S3 renvoie l'en-tête `x-amz-replication-status` dans la réponse :

- Lorsque vous demandez un objet depuis le compartiment source, Amazon S3 renvoie l'en-tête `x-amz-replication-status` si l'objet demandé peut être répliqué.

  Par exemple, imaginons que vous spécifiez le préfixe d'objet `TaxDocs` dans votre configuration de réplication pour indiquer à Amazon S3 de ne répliquer que les objets dotés du préfixe de nom de clé `TaxDocs`. Tous les objets que vous chargez ayant ce préfixe de nom de clé (par exemple, `TaxDocs/document1.pdf`) seront répliqués. Pour les demandes d'objet avec ce préfixe de nom de clé, Amazon S3 renvoie l'en-tête `x-amz-replication-status` avec l'une des valeurs suivantes pour le statut de réplication de l'objet : `PENDING`, `COMPLETED` ou `FAILED`.

  > **Note**
  >
  > Si la réplication d'objet échoue après avoir chargé un objet, vous ne pouvez pas relancer la réplication. Vous devez charger à nouveau l'objet ou utiliser la réplication par lot S3 pour répliquer tous les objets défaillants. Pour plus d'informations sur l'utilisation de la réplication par lot, consultez the section called "Réplication d'objets existants".
  > Les objets passent à un `FAILED` état pour des problèmes tels que l'absence d'autorisations de rôle de réplication, d'autorisations AWS Key Management Service (AWS KMS) ou d'autorisations de compartiment. Pour les échecs temporaires, par exemple si un compartiment ou une région n'est pas disponible, le statut de réplication ne passe pas à `FAILED`, mais reste `PENDING`. Une fois la ressource remise en ligne, Amazon S3 reprend la réplication de ces objets.

- Lorsque vous demandez un objet à partir du compartiment de destination, si l'objet demandé est un réplica créé par Amazon S3, Amazon S3 renvoie l'en-tête `x-amz-replication-status` avec la valeur `REPLICA`.

> **Note**
>
> Avant de supprimer un objet d'un compartiment source pour lequel la réplication a été activée, contrôlez le statut de réplication de l'objet pour vous assurer qu'il a été répliqué.

Si une configuration du cycle de vie S3 est activée sur le compartiment source, Amazon S3 interrompt les actions de cycle de vie tant que le statut des objets n'est pas marqué comme `COMPLETED` ou `FAILED`.

Statut de la réplication en cas de réplication vers plusieurs compartiments de destination

Lorsque vous répliquez des objets vers plusieurs compartiments de destination, l'en-tête `x-amz-replication-status` agit différemment. L'en-tête de l'objet source renvoie la valeur `COMPLETED` seulement quand la réplication a réussi vers toutes les destinations. L'en-tête reste à la valeur `PENDING` jusqu'à ce que la réplication soit terminée pour toutes les destinations. Si la réplication échoue vers une ou plusieurs destinations, l'en-tête renvoie `FAILED`.

Statut de la réplication si la synchronisation des modifications de réplica Simple Storage Service (Amazon S3) est activée

Lorsque vos règles de réplication activent la synchronisation des modifications de réplica Simple Storage Service (Amazon S3), les statuts des réplicas peuvent être différents de `REPLICA`. Si des modifications de métadonnées sont en cours de réplication, l'en-tête `x-amz-replication-status` renvoie `PENDING`. Si la synchronisation des modifications du réplica ne parvient pas à répliquer les métadonnées, l'en-tête renvoie `FAILED`. Si les métadonnées sont répliquées correctement, les réplicas retournent l'en-tête `REPLICA`.

Utilisation des informations de statut de réplication avec les tâches de réplication par lot

Lors de la création d'une tâche de réplication par lot, vous pouvez éventuellement spécifier des filtres supplémentaires, tels que la date de création d'objet et le statut de réplication, afin de réduire la portée de la tâche.

Vous pouvez filtrer les objets à répliquer sur la base de la valeur `ObjectReplicationStatuses`, en fournissant une ou plusieurs des valeurs suivantes :

- `"NONE"` – Indique qu'Amazon S3 n'a jamais tenté de répliquer l'objet auparavant.
- `"FAILED"` – Indique qu'Amazon S3 a déjà tenté mais n'a pas réussi à répliquer l'objet.
- `"COMPLETED"` – Indique qu'Amazon S3 a déjà répliqué l'objet avec succès.
- `"REPLICA"` – Indique qu'il s'agit d'un objet de réplica répliqué par Amazon S3 à partir d'une autre source.

Pour plus d'informations sur l'utilisation de ces valeurs de statut de réplication avec la réplication par lot, consultez the section called "Filtres pour une tâche de réplication par lot".

Recherche du statut de réplication

Pour obtenir le statut de réplication des objets dans un compartiment, utilisez l'outil d'inventaire Amazon S3. Amazon S3 envoie un fichier CSV au compartiment de destination que vous spécifiez dans la configuration d'inventaire. Vous pouvez également utiliser Amazon Athena pour interroger le statut de réplication dans le rapport d'inventaire. Pour plus d'informations sur l'inventaire Amazon S3, consultez Catalogage et analyse de vos données avec l'inventaire S3.

Vous pouvez également connaître l'état de réplication de l'objet à l'aide de la console Amazon S3, du AWS Command Line Interface (AWS CLI) ou du AWS SDK.

Utilisation de la console S3

Dans la console Amazon S3, vous pouvez afficher le statut de réplication d'un objet sur la page des détails de l'objet.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments à usage général, choisissez le nom du compartiment source de réplication.
4. Dans la liste Objets, sélectionnez le nom de l'objet. La page de détails de l'objet s'affiche.
5. Dans l'onglet Propriétés, faites défiler l'affichage vers le bas jusqu'à la section Présentation de la gestion des objets. Sous Configurations de gestion, lisez la valeur sous Statut de réplication.

À l'aide du AWS CLI

Utilisez la `head-object` commande AWS Command Line Interface (AWS CLI) pour récupérer les métadonnées de l'objet, comme indiqué dans l'exemple suivant. Remplacez le *`amzn-s3-demo-source-bucket1`* par le nom de votre compartiment source de réplication et remplacez les autres *`user input placeholders`* par vos propres informations.

```
aws s3api head-object --bucket amzn-s3-demo-source-bucket1 --key object-key --version-id object-version-id
```

La commande renvoie les métadonnées de l'objet, y compris `ReplicationStatus` comme illustré dans l'exemple de réponse suivant.

```
{
   "AcceptRanges":"bytes",
   "ContentType":"image/jpeg",
   "LastModified":"Mon, 23 Mar 2015 21:02:29 GMT",
   "ContentLength":3191,
   "ReplicationStatus":"COMPLETED",
   "VersionId":"jfnW.HIMOfYiD_9rGbSkmroXsFj3fqZ.",
   "ETag":"\"6805f2cfc46c0f04559748bb039d69ae\"",
   "Metadata":{

   }
}
```

À l'aide du AWS SDKs

Les fragments de code suivants obtiennent l'état de votre réplication à l'aide des AWS SDK pour Java touches et AWS SDK pour .NET, respectivement.

Java

```
GetObjectMetadataRequest metadataRequest = new GetObjectMetadataRequest(bucketName,
 key);
ObjectMetadata metadata = s3Client.getObjectMetadata(metadataRequest);

System.out.println("Replication Status : " +
 metadata.getRawMetadataValue(Headers.OBJECT_REPLICATION_STATUS));
```

.NET

```
GetObjectMetadataRequest getmetadataRequest = new GetObjectMetadataRequest
    {
         BucketName = sourceBucket,
         Key        = objectKey
    };

GetObjectMetadataResponse getmetadataResponse =
 client.GetObjectMetadata(getmetadataRequest);
Console.WriteLine("Object replication status: {0}",
 getmetadataResponse.ReplicationStatus);
```

Gestion du trafic multirégional avec des points d'accès multirégionaux

Les points d'accès multirégionaux Amazon S3 fournissent un point de terminaison global que les applications peuvent utiliser pour traiter les demandes provenant de compartiments S3 situés dans plusieurs Régions AWS. Vous pouvez utiliser des points d'accès multi-régions pour créer des applications multi-régions avec la même architecture utilisée dans une seule région, puis exécuter ces applications partout dans le monde. Au lieu d'envoyer les demandes sur l'Internet public encombré, les points d'accès multirégionaux offrent une résilience de réseau intégrée avec une accélération des demandes basées sur Internet vers Amazon S3. Les demandes d'application adressées à un point d'accès global multirégional sont utilisées AWS Global Acceleratorpour acheminer automatiquement sur le réseau AWS mondial le compartiment S3 le plus proche ayant un statut de routage actif.

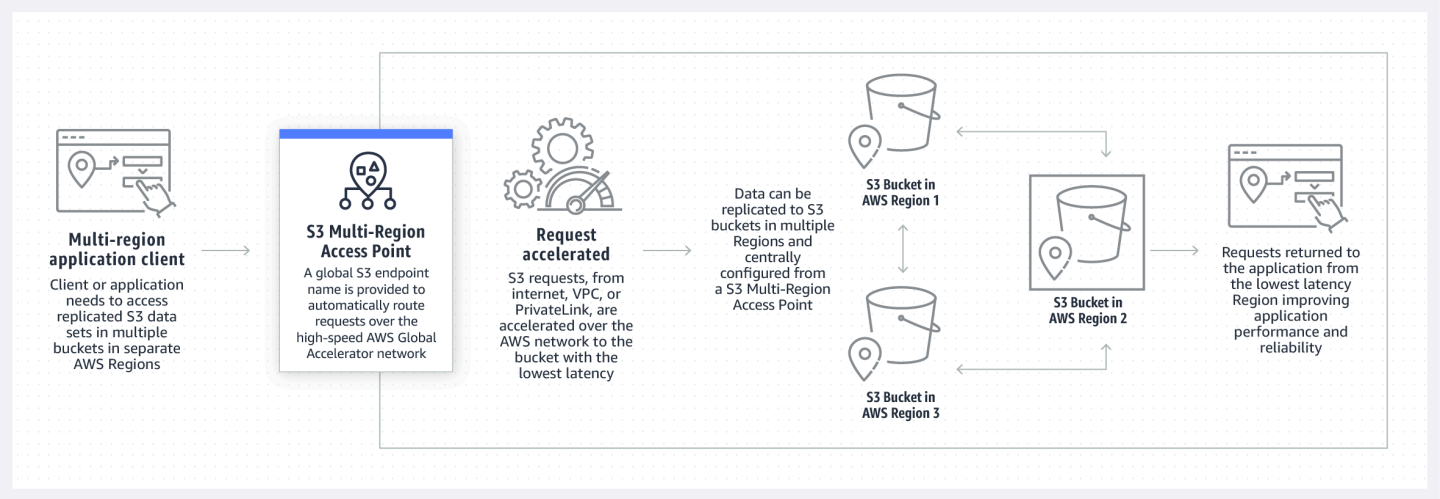
En cas d'interruption du trafic régional, vous pouvez utiliser les contrôles de basculement des points d'accès multirégionaux pour déplacer le trafic de demandes de données S3 entre les deux Régions AWS et rediriger le trafic S3 hors des perturbations en quelques minutes. Vous pouvez également tester la résilience des applications face à une interruption pour réaliser le basculement des applications et effectuer des simulations de reprise après sinistre. Si vous devez connecter et accélérer les demandes adressées à S3 depuis l'extérieur d'un VPC, vous pouvez simplifier les applications et l'architecture réseau avec les points d'accès multirégionaux Amazon S3. Vos demandes de points d'accès multirégionaux seront acheminées via le réseau AWS mondial, puis renvoyées vers S3 au sein du réseau Région AWS, sans avoir à passer par l'Internet public. Par conséquent, vous pouvez créer des applications à plus haute disponibilité.

Lors de la création et de la configuration de vos points d'accès multirégionaux, vous spécifierez un ensemble d'emplacements dans Régions AWS lesquels vous souhaitez stocker les données à diffuser via ce point d'accès multirégional. Vous pouvez utiliser le nom de point de terminaison des points d'accès multirégionaux fourni pour connecter vos clients. Une fois que vous avez établi vos connexions client, vous pouvez sélectionner les compartiments existants ou nouveaux entre lesquels vous souhaitez router les demandes de points d'accès multirégionaux. Ensuite, utilisez les règles de réplication interrégionale (CRR) S3 pour synchroniser les données entre les compartiments de ces régions.

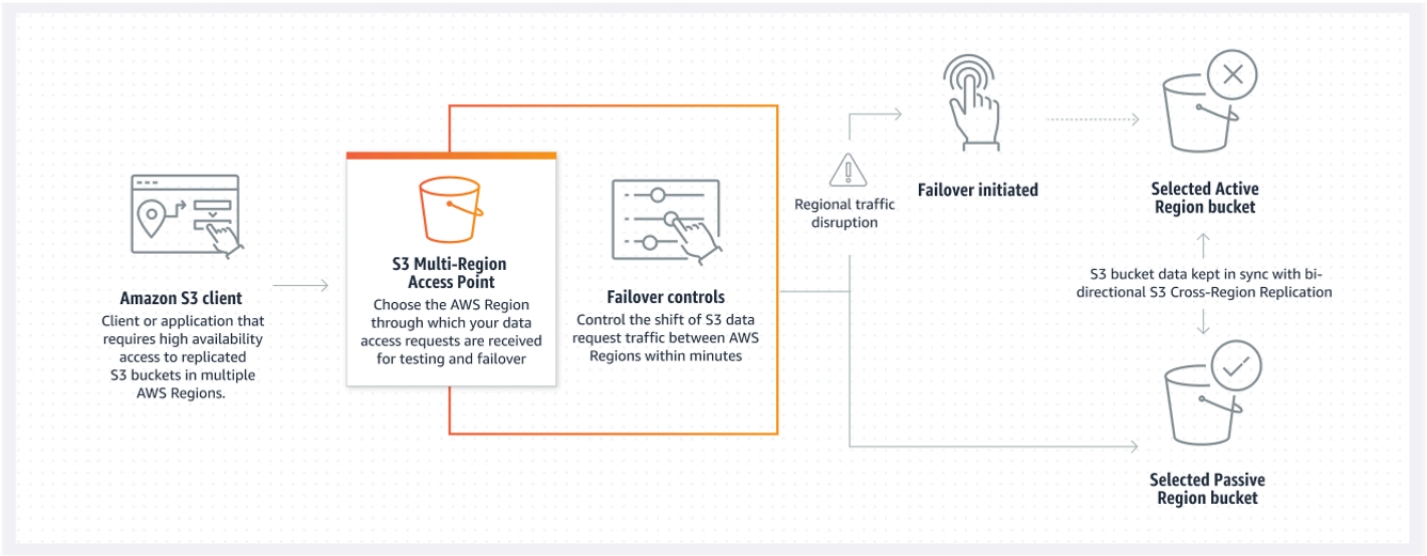
Une fois que vous avez configuré votre point d'accès multirégional, vous pouvez demander ou écrire des données via le point de terminaison global des points d'accès multirégionaux. Amazon S3 traite automatiquement les demandes du jeu de données répliqué à partir de la région disponible

la plus proche. Dans le AWS Management Console, vous pouvez également consulter la topologie de réplication sous-jacente et les mesures de réplication liées à vos demandes de points d'accès multirégionaux. Cela vous permet de créer, de gérer et de surveiller encore plus facilement le stockage pour les applications multirégionales. Vous pouvez également utiliser Amazon CloudFront pour automatiser la création et la configuration des points d'accès multirégionaux S3.

L'image suivante est une représentation graphique d'un point d'accès multi-régions Amazon S3 dans une configuration active-active. Le graphique montre comment les demandes Amazon S3 sont automatiquement acheminées vers les compartiments de la Région AWS active la plus proche.



L'image suivante est une représentation graphique d'un point d'accès multi-régions Amazon S3 dans une configuration active-passive. Le graphique montre comment vous pouvez contrôler le trafic d'accès aux données d'Amazon S3 pour basculer entre une Régions AWS active et passive.



Pour plus d'informations sur l'utilisation des points d'accès multi-régions, consultez Didacticiel : Débuter à l'aide des points d'accès multi-régions Amazon S3.

Rubriques

- Création de points d'accès multi-Régions
- Configurer un point d'accès multi-Régions pour utilisation avec AWS PrivateLink
- Effectuer des requêtes par l'intermédiaire d'un point d'accès multi-régions

Création de points d'accès multi-Régions

Pour créer un point d'accès multi-régions Amazon S3, procédez comme suit :

- Spécifiez le nom du point d'accès multi-régions.
- Choisissez un compartiment dans chaque compartiment dans Région AWS lequel vous souhaitez répondre aux demandes du point d'accès multirégional.
- Configurez les paramètres de blocage de l'accès public Amazon S3 pour le point d'accès multi-régions.

Vous fournissez toutes cces informations dans une demande de création, qu'Amazon S3 traite de manière asynchrone. Amazon S3 fournit un jeton que vous pouvez utiliser pour surveiller l'état de la demande de création asynchrone.

Veillez à résoudre les avertissements de sécurité, les erreurs, les avertissements généraux et les suggestions provenant d' AWS Identity and Access Management Access Analyzer avant d'enregistrer votre stratégie. IAM Access Analyzer exécute des vérifications de politiques pour valider votre politique par rapport à la grammaire de politique et aux bonnes pratiques IAM. Ces vérifications génèrent des résultats et fournissent des recommandations exploitables pour vous aider à créer des stratégies fonctionnelles et conformes aux bonnes pratiques en matière de sécurité. Pour en savoir plus sur la validation des politiques à l'aide d'IAM Access Analyzer, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisateur IAM. Pour afficher la liste des avertissements, erreurs et suggestions renvoyés par IAM Access Analyzer, consultez la Référence de vérification de stratégie IAM Access Analyzer.

Lorsque vous utilisez l'API, la demande de création d'un point d'accès multi-Régions est asynchrone. Lorsque vous soumettez une demande de création d'un point d'accès multi-Régions, Amazon S3 autorise la demande de manière synchrone. Il renvoie ensuite immédiatement un jeton que vous

pouvez utiliser pour suivre la progression de la demande de création. Pour en savoir plus sur le suivi des demandes asynchrones pour créer et gérer des points d'accès multi-Régions, consultez Utilisation de points d'accès multi-régions avec des opérations d'API prises en charge.

Après avoir créé le point d'accès multi-Régions, vous pourrez créer une politique de contrôle d'accès pour celui-ci. Chaque point d'accès multi-Régions peut être associé à une politique. Une politique de point d'accès multi-régions est une politique basée sur les ressources qui vous permet de limiter l'utilisation du point d'accès multi-régions par ressource, utilisateur ou autres conditions.

> **Note**
>
> Pour qu'une application ou un utilisateur puisse accéder à un objet via un point d'accès multi-régions, les deux stratégies suivantes doivent autoriser la demande :
>
> - La stratégie d'accès associée au point d'accès multi-régions
> - La stratégie d'accès pour le compartiment sous-jacent qui contient l'objet
>
> Lorsque les deux politiques sont différentes, la politique la plus restrictive a la priorité. Pour simplifier la gestion des autorisations pour les points d'accès multi-régions, vous pouvez déléguer le contrôle d'accès du compartiment au point d'accès multi-régions. Pour de plus amples informations, veuillez consulter the section called "Exemples de politique de point d'accès multi-régions".

L'utilisation d'un compartiment avec un point d'accès multi-régions ne modifie pas le comportement du compartiment si le compartiment est accessible via le nom de compartiment existant ou un nom Amazon Resource Name (ARN). Toutes les opérations existantes sur le compartiment continuent de fonctionner comme auparavant. Les restrictions que vous incluez dans une politique de point d'accès s'appliquent uniquement aux demandes effectuées via ce point d'accès.

Vous pouvez mettre à jour la politique pour un point d'accès multi-Régions après l'avoir créée, mais vous ne pouvez pas la supprimer. Vous pouvez toutefois mettre à jour la politique de point d'accès multi-régions pour refuser toutes les autorisations.

Rubriques

- Règles relatives à l'attribution de noms pour les points d'accès multi-Régions Amazon S3
- Règles de sélection des compartiments pour les points d'accès multi-Régions Amazon S3

- Création d'un point d'accès multi-régions Amazon S3
- Bloquer l'accès public à l'aide des points d'accès multi-Régions Amazon S3
- Affichage des détails de la configuration des points d'accès multi-régions Amazon S3
- Suppression d'un point d'accès multi-régions

Règles relatives à l'attribution de noms pour les points d'accès multi-Régions Amazon S3

Lorsque vous créez un point d'accès multi-Régions, vous lui attribuez un nom, qui est une chaîne que vous choisissez. Vous ne pourrez pas modifier le nom du point d'accès multi-Régions après sa création. Le nom doit être unique dans votre Compte AWS, et il doit être conforme aux exigences de dénomination répertoriées dans Restrictions et limitations des points d'accès multi-régions. Pour vous aider à identifier le point d'accès multi-Régions, utilisez un nom significatif pour vous, pour votre organisation ou qui reflète le scénario.

Vous utiliserez ce nom lors de l'appel d'opérations de gestion de points d'accès multi-Régions, telles que `GetMultiRegionAccessPoint` et `PutMultiRegionAccessPointPolicy`. Le nom n'est pas utilisé pour envoyer des demandes au point d'accès multi-régions, et il n'est pas nécessaire de l'exposer aux clients qui effectuent des demandes à l'aide du point d'accès multi-régions.

Quand Amazon S3 crée un point d'accès multi-Régions, il lui attribue automatiquement un alias. Cet alias est une chaîne alphanumérique unique qui se termine par `.mrap`. L'alias est utilisé pour créer le nom d'hôte et le nom Amazon Resource Name (ARN) d'un point d'accès multi-Régions. Le nom complet est également basé sur l'alias du point d'accès multi-Régions.

Vous ne pouvez pas déterminer le nom d'un point d'accès multi-Régions à partir de son alias, de sorte que vous pouvez divulguer un alias sans risque d'exposer le nom, l'objectif ou le propriétaire du point d'accès multi-Régions. Amazon S3 sélectionne l'alias pour chaque nouveau point d'accès multi-Régions et l'alias ne peut pas être modifié. Pour en savoir plus sur le traitement d'un point d'accès multi-Régions, consultez Effectuer des requêtes par l'intermédiaire d'un point d'accès multi-régions.

Les alias de points d'accès multi-Régions sont uniques dans le temps et ne sont pas basés sur le nom ou sur la configuration d'un point d'accès multi-Régions. Si vous créez un point d'accès multi-Régions, puis le supprimez et en créez un autre portant le même nom et ayant la même configuration, le deuxième point d'accès multi-Régions aura un alias différent du premier. Les nouveaux points d'accès multi-Régions ne peuvent jamais avoir le même alias qu'un point d'accès multi-Régions précédent.

Règles de sélection des compartiments pour les points d'accès multi-Régions Amazon S3

Chaque point d'accès multi-Régions est associé aux Régions où vous souhaitez traiter les demandes. Le point d'accès multi-Régions doit être associé à exactement un compartiment dans chacune de ces Régions. Vous indiquez le nom de chaque compartiment dans la demande de création du point d'accès multi-Régions. Les compartiments qui prennent en charge le point d'accès multirégional peuvent se trouver soit dans le même Compte AWS que celui qui possède le point d'accès multirégional, soit dans un autre. Comptes AWS

Un seul compartiment peut être utilisé par plusieurs points d'accès multi-Régions.

Important

- Vous pouvez indiquer les compartiments associés à un point d'accès multi-Régions uniquement au moment de sa création. Une fois créé, vous ne pourrez pas ajouter, modifier ou supprimer des compartiments de la configuration de point d'accès multi-Régions. Pour modifier les compartiments, vous devrez supprimer tout le point d'accès multi-Régions et en créer un autre.
- Vous ne pouvez pas supprimer un compartiment qui fait partie d'un point d'accès multi-Régions. Si vous souhaitez supprimer un compartiment attaché à un point d'accès multi-régions, supprimez d'abord le point d'accès multi-régions.
- Si vous ajoutez un compartiment qui appartient à un autre compte à votre point d'accès multi-régions, le propriétaire doit également mettre à jour sa politique de compartiment pour accorder des autorisations sur le point d'accès multi-régions. Sinon, le point d'accès multi-régions ne sera pas en mesure de récupérer les données de ce compartiment. Pour des exemples de politiques indiquant comment accorder un tel accès, consultez Exemples de politique de point d'accès multi-régions.
- Les Régions ne prennent pas toutes en charge les points d'accès multi-Régions. Pour obtenir la liste des Régions de prise en charge, consultez Restrictions et limitations des points d'accès multi-régions.

Vous pouvez créer des règles de réplication pour synchroniser les données entre les compartiments. Ces règles vous permettent de copier automatiquement les données des compartiments source vers des compartiments de destination. Le fait d'avoir des compartiments connectés à un point d'accès

multi-Régions n'affecte pas le fonctionnement de la réplication. La configuration de la réplication avec des points d'accès multi-Régions est décrite dans une section ultérieure.

> **Important**
>
> Lorsque vous effectuez une demande à un point d'accès multi-régions, le point d'accès multi-régions ne connaît pas le contenu des compartiments dans le point d'accès multi-régions. Par conséquent, le compartiment qui reçoit la demande peut ne pas contenir les données demandées. Pour créer des jeux de données cohérents dans les compartiments Amazon S3 associés à un point d'accès multi-régions, nous vous recommandons de configurer la réplication entre régions (CRR) S3. Pour de plus amples informations, veuillez consulter Configuration de la réplication à utiliser avec des points d'accès multi-régions.

Création d'un point d'accès multi-régions Amazon S3

L'exemple suivant montre comment créer un point d'accès multi-régions à l'aide de la console Amazon S3.

Utilisation de la console S3

Créer un point d'accès multi-Régions

> **Note**
>
> Les régions optionnelles aux points d'accès multirégionaux ne sont actuellement pas prises en charge dans la console Amazon S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Choisissez Créer des points d'accès multi-régions pour commencer à créer votre point d'accès multi-régions.
4. Sur la page Point d'accès multi-régions, indiquez un nom pour le point d'accès multi-régions dans le champ Nom du point d'accès multi-régions.

5. Sélectionnez les compartiments qui seront associés à ce point d'accès multi-régions. Vous pouvez choisir des compartiments qui se trouvent dans votre compte ou choisir des compartiments provenant d'autres comptes.

> **Note**
>
> Vous devez ajouter au moins un compartiment à partir de votre compte ou d'autres comptes. Sachez également que les points d'accès multi-régions ne prennent en charge qu'un seul compartiment par Région AWS. Par conséquent, vous ne pouvez pas ajouter deux compartiments de la même région. Les Régions AWS désactivées par défaut ne sont pas prises en charge.

- Pour ajouter un compartiment qui se trouve dans votre compte, choisissez Ajouter des compartiments. Une liste de tous les compartiments de votre compte s'affiche. Vous pouvez rechercher votre compartiment par nom ou trier les noms des compartiments par ordre alphabétique.
- Pour ajouter un compartiment à partir d'un autre compte, choisissez Ajouter un compartiment à partir d'autres comptes. Assurez-vous de connaître le nom et l' Compte AWS identifiant exacts du compartiment, car vous ne pouvez pas rechercher ou rechercher des compartiments dans d'autres comptes.

> **Note**
>
> Vous devez saisir un Compte AWS identifiant et un nom de compartiment valides. Le compartiment doit également se trouver dans une région prise en charge, sinon vous rencontrerez une erreur lorsque vous tenterez de créer votre point d'accès multi-régions. Pour obtenir la liste des régions qui prennent en charge les points d'accès multi-régions, consultez Restrictions et limitations des points d'accès multi-régions.

6. (Facultatif) Si vous devez supprimer un compartiment que vous avez ajouté, choisissez Supprimer.

> **Note**
>
> Vous ne pouvez pas ajouter ni supprimer de compartiments à ce point d'accès multi-régions une fois que vous avez fini de le créer.

7. Sous Paramètres de blocage de l'accès public à ce point d'accès multi-Régions, sélectionnez les paramètres de blocage de l'accès public que vous souhaitez appliquer au point d'accès multi-Régions. Tous les paramètres de blocage de l'accès public sont activés par défaut pour les points d'accès. Nous vous recommandons de laisser tous les paramètres activés, sauf si vous savez que vous avez un besoin spécifique de désactiver l'un d'entre eux.

   > **Note**
   >
   > Vous ne pouvez pas modifier les paramètres de blocage de l'accès public après la création du point d'accès multi-régions. Par conséquent, si vous avez l'intention de bloquer l'accès public, assurez-vous que vos applications fonctionnent correctement sans accès public avant de créer un point d'accès multi-régions.

8. Choisissez Créer un point d'accès multi-Régions.

> **Important**
>
> Quand vous ajoutez un compartiment qui appartient à un autre compte à votre point d'accès multi-régions, le propriétaire doit également mettre à jour sa politique de compartiment pour accorder des autorisations sur le point d'accès multi-régions. Sinon, le point d'accès multi-régions ne sera pas en mesure de récupérer les données de ce compartiment. Pour des exemples de politiques indiquant comment accorder un tel accès, consultez Exemples de politique de point d'accès multi-régions.

À l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour créer un point d'accès multirégional. Lorsque vous créez le point d'accès multi-régions, vous devez indiquer tous les compartiments qu'il devra prendre en charge. Vous ne pouvez pas ajouter des compartiments au point d'accès multi-régions après sa création.

L'exemple suivant crée un point d'accès multi-régions avec deux compartiments à l'aide de l' AWS CLI. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

> **Note**
>
> Pour créer un point d'accès multirégional à l'aide de buckets dans une région optionnelle, assurez-vous d'activer d'abord toutes les régions optionnelles. Dans le cas contraire, vous recevrez un `403 InvalidRegion` message d'erreur lorsque vous tenterez de créer un point d'accès multirégional à l'aide de compartiments pour une région à laquelle vous n'avez pas encore souscrit.

```
aws s3control create-multi-region-access-point --account-id 111122223333 --details '{
        "Name": "simple-multiregionaccesspoint-with-two-regions",
        "PublicAccessBlock": {
            "BlockPublicAcls": true,
            "IgnorePublicAcls": true,
            "BlockPublicPolicy": true,
            "RestrictPublicBuckets": true
        },
        "Regions": [
            { "Bucket": "amzn-s3-demo-bucket1" },
            { "Bucket": "amzn-s3-demo-bucket2" }
        ]
    }' --region us-west-2
```

Bloquer l'accès public à l'aide des points d'accès multi-Régions Amazon S3

Chaque point d'accès multi-Régions dispose de paramètres distincts pour bloquer l'accès public Amazon S3. Ces paramètres fonctionnent conjointement avec les paramètres de blocage de l'accès public pour le Compte AWS propriétaire du point d'accès multirégional et des compartiments sous-jacents.

Quand Amazon S3 autorise une demande, il applique la combinaison la plus restrictive de ces paramètres. Si les paramètres de blocage de l'accès public pour l'une de ces ressources (le compte propriétaire du point d'accès multi-régions, le compartiment sous-jacent ou le compte propriétaire du compartiment) bloquent l'accès à l'action ou à la ressource demandée, Amazon S3 rejettera la demande.

Nous vous recommandons d'activer tous les paramètres de blocage de l'accès public sauf si vous devez spécifiquement en désactiver certains. Tous les paramètres de blocage de l'accès public sont activés par défaut pour les points d'accès. Si l'option de blocage de l'accès public est activée, le point d'accès multi-régions ne peut pas accepter les demandes basées sur Internet.

> **Important**
>
> Vous ne pouvez pas modifier les paramètres de blocage de l'accès public après la création du point d'accès multi-régions.

Pour en savoir plus sur le blocage de l'accès public Amazon S3, consultez Blocage de l'accès public à votre stockage Amazon S3.

Affichage des détails de la configuration des points d'accès multi-régions Amazon S3

L'exemple suivant montre comment afficher les détails de la configuration d'un point d'accès multi-régions à l'aide de la console Amazon S3.

Utilisation de la console S3

Créer un point d'accès multi-Régions

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Choisissez le nom du point d'accès multi-régions dont vous souhaitez afficher les détails de la configuration.

   - L'onglet Propriétés répertorie tous les compartiments associés à votre point d'accès multi-régions, la date de création, l'Amazon Resource Name (ARN) et l'alias. La colonne ID de Compte AWS répertorie également tous les compartiments appartenant à des comptes externes associés à votre point d'accès multi-régions.
   - L'onglet Autorisations répertorie les paramètres de blocage d'accès public appliqués aux compartiments associés à ce point d'accès multi-régions. Vous pouvez également afficher la politique de point d'accès multi-régions, si vous en avez créé une. L'alerte Infos sur la page Autorisations répertorie également tous les compartiments (de votre compte et d'autres comptes) pour ce point d'accès multi-régions pour lesquels le paramètre L'accès public est bloqué est activé.
   - L'onglet Réplication et basculement fournit une vue cartographique des compartiments associés à votre point d'accès multi-régions et des régions dans lesquelles se trouvent les compartiments. S'il existe des compartiments provenant d'un autre compte dont vous n'êtes

pas autorisé à extraire des données, la région sera marquée en rouge sur la carte Récapitulatif de réplication, ce qui indique qu'il s'agit d'une Région AWS présentant des erreurs lors de l'obtention du statut de réplication.

> **Note**
>
> Pour récupérer les informations sur le statut de réplication d'un compartiment dans un compte externe, le propriétaire du compartiment doit vous accorder l'autorisation `s3:GetBucketReplication` conformément à sa politique en matière de compartiment.

Cet onglet fournit également les métriques de réplication, les règles de réplication et les statuts de basculement pour les régions utilisées avec votre point d'accès multi-régions.

À l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour afficher les détails de configuration d'un point d'accès multirégional.

L' AWS CLI exemple suivant montre la configuration actuelle de votre point d'accès multirégional. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control get-multi-region-access-point --account-id 111122223333 --name amzn-s3-demo-bucket
```

Suppression d'un point d'accès multi-régions

La procédure suivante montre comment supprimer un point d'accès multi-régions à l'aide de la console Amazon S3. Sachez que la suppression d'un point d'accès multirégional ne supprime pas les compartiments associés au point d'accès multirégional. Au lieu de cela, il supprime uniquement le point d'accès multirégional lui-même.

> **Note**
>
> Les points d'accès multirégionaux S3 utilisant des buckets dans des régions AWS optionnelles ne sont actuellement pris en charge que par AWS SDKs le biais de la CLI. AWS

Pour supprimer un point d'accès multirégional à l'aide de compartiments situés dans une région optionnelle, assurez-vous de spécifier les régions AWS facultatives que votre compte peut utiliser en premier. Dans le cas contraire, si vous essayez de supprimer un point d'accès multirégional qui utilise des compartiments dans des régions où l' AWS option d'inscription est désactivée, vous recevrez un message d'erreur.

Utilisation de la console S3

Pour supprimer un point d'accès multi-régions

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Sélectionnez le bouton d'option en regard du nom de votre point d'accès multi-régions.
4. Sélectionnez Delete (Supprimer).
5. Dans la boîte de dialogue Supprimer le point d'accès multirégional, entrez le nom du AWS compartiment que vous souhaitez supprimer.

   > **Note**
   >
   > Assurez-vous de saisir un nom de compartiment valide. Dans le cas contraire, le bouton Supprimer sera désactivé.

6. Choisissez Supprimer pour confirmer la suppression de votre point d'accès multi-régions.

À l'aide du AWS CLI

Vous pouvez utiliser le AWS CLI pour supprimer un point d'accès multirégional. L'action ne supprime pas les compartiments associés au point d'accès multi-régions, mais uniquement le point d'accès multi-régions. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control delete-multi-region-access-point --account-id 123456789012 --details
 Name=example-multi-region-access-point-name
```

Configurer un point d'accès multi-Régions pour utilisation avec AWS PrivateLink

Vous pouvez utiliser les points d'accès multi-régions pour acheminer le trafic de demandes Amazon S3 entre plusieurs Régions AWS. Chaque point d'accès multi-régions achemine le trafic de demandes de données Amazon S3 depuis plusieurs sources sans que vous ayez à créer des configurations réseau complexes avec des points de terminaison distincts. Ces sources de trafic de demandes de données incluent :

- Trafic provenant d'un cloud privé virtuel (VPC)
- Trafic provenant des centres de données sur site transitant par AWS PrivateLink
- Trafic provenant de l'Internet public

Si vous établissez une AWS PrivateLink connexion à un point d'accès multirégional S3, vous pouvez acheminer les demandes S3 vers AWS, ou entre plusieurs Régions AWS, via une connexion privée en utilisant une architecture et une configuration réseau simples. Lorsque vous l'utilisez AWS PrivateLink, il n'est pas nécessaire de configurer une connexion d'appairage VPC.

Rubriques

- Configuration des régions optionnelles aux points d'accès multirégionaux
- Configurer un point d'accès multi-Régions pour utilisation avec AWS PrivateLink
- Supprimer l'accès à un point d'accès multi-Régions à partir d'un point de terminaison d'un VPC

Configuration des régions optionnelles aux points d'accès multirégionaux

Une région AWS optionnelle est une région qui n'est pas activée par défaut dans votre AWS compte. En revanche, les régions activées par défaut sont appelées Régions AWS régions commerciales.

Pour commencer à utiliser les points d'accès multirégionaux dans les régions AWS optionnelles, vous devez activer manuellement la région optionnelle pour votre AWS compte avant de créer votre point d'accès multirégional. Après avoir activé la région optionnelle, vous pouvez créer des points d'accès multirégionaux avec des buckets dans la région optionnelle sélectionnée. Pour savoir comment activer ou désactiver une région optionnelle pour votre AWS compte ou votre AWS organisation, voir Activer ou désactiver une région pour les comptes autonomes ou Activer ou désactiver une région dans votre organisation.

> **Note**
>
> Les régions optionnelles aux points d'accès multirégionaux ne sont actuellement prises en charge que via AWS SDKs et. AWS CLI

Les points d'accès multirégionaux S3 prennent en charge les régions AWS optionnelles suivantes :

- `Africa (Cape Town)`
- `Asia Pacific (Hong Kong)`
- `Asia Pacific (Jakarta)`
- `Asia Pacific (Melbourne)`
- `Asia Pacific (Hyderabad)`
- `Canada West (Calgary)`
- `Europe (Zurich)`
- `Europe (Milan)`
- `Europe (Spain)`
- `Israel (Tel Aviv)`
- `Middle East (Bahrain)`
- `Middle East (UAE)`

> **Note**
>
> L'activation d'une région optionnelle n'entraîne aucun coût supplémentaire. Cependant, la création ou l'utilisation d'une ressource dans un point d'accès multirégional entraîne des frais de facturation.

Utilisation d'un point d'accès multirégional dans une région AWS optionnelle

Pour effectuer une opération de plan de données sur votre point d'accès multirégional, tous les AWS comptes associés doivent activer les régions facultatives qui font partie du point d'accès multirégional. Cette exigence s'applique au compte du demandeur, au propriétaire du point d'accès multirégional, aux propriétaires du compartiment S3 et au propriétaire du point de terminaison VPC. Si l'un de ces comptes n'active pas les régions AWS optionnelles, les demandes de point

d'accès multirégional échouent. Pour plus d'informations sur les `AllAccessDisabled` erreurs `InvalidToken` ou, consultez la section Liste des codes d'erreur.

> **Note**
>
> Les opérations du plan de contrôle, telles que la mise à jour de votre politique de point d'accès multirégional ou la mise à jour de votre configuration de basculement, ne sont pas affectées par le statut de région opt-in des régions faisant partie de votre point d'accès multirégional. Il n'est pas non plus nécessaire de désactiver les régions optionnelles actives avant de supprimer un point d'accès multirégional.

Désactivation d'une région AWS opt-in active

Si vous désactivez la région opt-in qui fait partie de votre point d'accès multirégional, les demandes acheminées vers cette région génèrent une erreur. `403 AllAccessDisabled` Pour désactiver en toute sécurité une région optionnelle, nous vous recommandons d'abord d'identifier une autre région dans la configuration de votre point d'accès multirégional vers laquelle acheminer le trafic. Vous pouvez ensuite utiliser les commandes de basculement des points d'accès multirégionaux pour marquer la région alternative comme active et marquer la région à désactiver comme passive. Après avoir modifié les commandes de basculement, vous pouvez désactiver la région dont vous souhaitez vous désinscrire.

Activation d'une région AWS opt-in précédemment désactivée

Pour activer une AWS région optionnelle qui était précédemment désactivée pour votre point d'accès multirégional, assurez-vous de mettre à jour les paramètres de votre AWS compte. Après avoir réactivé la région opt-in, exécutez l'opération PutMultiRegionAccessPointPolicyAPI pour appliquer la politique des points d'accès multirégionaux à la région optionnelle.

Si vous accédez à votre point d'accès multirégional via un point de terminaison VPC, nous vous recommandons de mettre à jour votre politique VPCE et d'utiliser l'opération d'API pour appliquer ModifyVpcEndpointla politique de point de terminaison VPC mise à jour à la région optionnelle réactivée.

Politique relative aux points d'accès multirégionaux et comptes multiples AWS

Si votre politique de points d'accès multirégionaux accorde l'accès à plusieurs AWS comptes, tous les comptes demandeurs doivent également activer les mêmes régions optionnelles dans leurs paramètres de compte. Si le compte du demandeur soumet une demande de point d'accès

multirégional sans activer les régions facultatives qui font partie du point d'accès multirégional, cela provoquera une erreur. `400 InvalidToken`

AWS Considérations relatives à la région d'adhésion

Lorsque vous accédez à un point d'accès multirégional à partir d'une région optionnelle, tenez compte des points suivants :

- Lorsque vous activez une région optionnelle, elle vous permet de créer un point d'accès multirégional à l'aide des compartiments de la région optionnelle. Lorsque vous désactivez une région optionnelle, le point d'accès multirégional n'est plus pris en charge dans la région optionnelle. Si vous ne souhaitez plus activer de région optionnelle pour votre point d'accès multirégional, assurez-vous d'abord de désactiver la région pour votre compte. Créez ensuite un nouveau point d'accès multirégional avec votre liste préférée de régions facultatives.
- Si vous tentez de créer votre point d'accès multirégional avec une région opt-in désactivée, vous recevrez un `403 InvalidRegion` message d'erreur. Après avoir activé la région optionnelle, essayez de créer à nouveau le point d'accès multirégional.
- Le nombre maximum de régions prises en charge pour un point d'accès multirégional est de 17 régions. Cela inclut à la fois les régions optionnelles et les régions commerciales. Pour plus d'informations, consultez la section Restrictions et limitations relatives aux points d'accès multirégionaux.
- Les demandes de plan de contrôle pour les points d'accès multirégionaux fonctionneront, même si vous n'avez opté pour aucune région.
- Lorsque vous essayez de créer un point d'accès multirégional pour la première fois, vous devez opter pour toutes les régions qui font partie du point d'accès multirégional.
- Tous les AWS comptes autorisés à accéder à un point d'accès multirégional S3 par le biais de la politique de point d'accès multirégional doivent également activer les mêmes régions optionnelles qui font partie du point d'accès multirégional.

Configurer un point d'accès multi-Régions pour utilisation avec AWS PrivateLink

AWS PrivateLink vous fournit une connectivité privée à Amazon S3 à l'aide d'adresses IP privées dans votre cloud privé virtuel (VPC). Vous pouvez provisionner un ou plusieurs points de terminaison d'interface dans votre VPC pour vous connecter aux points d'accès multi-Régions Amazon S3.

Vous pouvez créer des points de terminaison com.amazonaws.s3-global.accesspoint pour les points d'accès multirégionaux via le, ou. AWS Management Console AWS CLI AWS SDKs Pour en savoir

plus sur la configuration d'un point de terminaison d'interface pour un point d'accès multi-Régions, consultez Points de terminaison d'un VPC d'interface dans le guide de l'utilisateur VPC.

Pour adresser des demandes à un point d'accès multi-Régions via des points de terminaison d'interface, procédez comme suit pour configurer le VPC et le point d'accès multi-Régions.

Pour configurer un point d'accès multirégional à utiliser avec AWS PrivateLink

1. Créez ou disposez d'un point de terminaison d'un VPC approprié qui peut se connecter à des points d'accès multi-Régions. Pour en savoir plus sur les points de terminaison d'un VPC, consultez Points de terminaison d'un VPC d'interface dans le guide de l'utilisateur VPC.

   > **Important**
   >
   > Veillez à créer un point de terminaison com.amazonaws.s3-global.accesspoint. Les autres types de points de terminaison ne peuvent pas accéder aux points d'accès multi-Régions.

   Après la création de ce point de terminaison d'un VPC, toutes les demandes de point d'accès multi-Régions dans le VPC seront acheminées via ce point de terminaison si vous disposez d'un DNS privé activé pour le point de terminaison. Cela est activé par défaut.
2. Si la politique de point d'accès multi-Régions ne prend pas en charge les connexions à partir des points de terminaison d'un VPC, vous devrez la mettre à jour.
3. Vérifiez que les politiques de compartiment individuelles autorisent l'accès aux utilisateurs du point d'accès multi-Régions.

N'oubliez pas que les points d'accès multi-Régions fonctionnent en acheminant les demandes vers des compartiments, non en les exécutant eux-mêmes. Il est important de s'en souvenir, car l'expéditeur de la demande doit disposer des autorisations sur le point d'accès multi-Régions et être autorisé à accéder aux compartiments individuels dans le point d'accès multi-Régions. Sinon, la demande risque d'être acheminée vers un compartiment où l'expéditeur n'a pas les autorisations nécessaires pour répondre à la demande. Un point d'accès multirégional et les compartiments associés peuvent appartenir au même compte ou à un autre AWS compte. Cependant, vous pouvez utiliser un point d'accès multirégional à VPCs partir de différents comptes si les autorisations sont correctement configurées.

Pour cette raison, la politique de point de terminaison d'un VPC doit autoriser l'accès au point d'accès multi-Régions et à chaque compartiment sous-jacent qui doit être capable de traiter les demandes. Par exemple, supposons que vous ayez un point d'accès multi-Régions avec l'alias `mfzwi23gnjvgw.mrap`. Il est soutenu par des compartiments `amzn-s3-demo-bucket1` et `amzn-s3-demo-bucket2` qui appartiennent tous deux à un compte AWS`123456789012`. Dans ce cas, la politique de point de terminaison VPC suivante permettrait que les demandes `GetObject` du VPC faites à `mfzwi23gnjvgw.mrap` soient satisfaites par l'un ou l'autre des compartiments de sauvegarde.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Read-buckets-and-MRAP-VPCE-policy",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "arn:aws:s3:::amzn-s3-demo-bucket2/*",
            "arn:aws:s3::111122223333:accesspoint/mfzwi23gnjvgw.mrap/object/*"
        ]
    }]
}
```

Comme mentionné précédemment, vous devez également vous assurer que la politique de point d'accès multi-Régions est configurée de manière à prendre en charge l'accès via un point de terminaison d'un VPC. Il n'est pas nécessaire de préciser le point de terminaison d'un VPC qui demande l'accès. L'exemple de politique suivant accorderait l'accès à tout demandeur essayant d'utiliser le point d'accès multi-régions pour les demandes `GetObject`.

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
    {
        "Sid": "Open-read-MRAP-policy",
        "Effect": "Allow",
        "Principal": "*",
        "Action": [
            "s3:GetObject"
          ],
        "Resource": "arn:aws:s3::111122223333:accesspoint/mfzwi23gnjvgw.mrap/
object/*"
    }]
}
```

Et, bien entendu, les compartiments individuels auraient chacun besoin d'une politique pour prendre en charge l'accès à partir des demandes soumises via le point de terminaison d'un VPC. L'exemple de politique suivant accorde l'accès en lecture à tous les utilisateurs anonymes, ce qui inclut les demandes effectuées via le point de terminaison VPC.

JSON

```
{
    "Version":"2012-10-17",
   "Statement": [
   {
       "Sid": "Public-read",
       "Effect":"Allow",
       "Principal": "*",
       "Action": "s3:GetObject",
       "Resource": [
           "arn:aws:s3:::amzn-s3-demo-bucket1",
           "arn:aws:s3:::amzn-s3-demo-bucket2/*"]
    }]
}
```

Pour en savoir plus sur la modification d'une politique de point de terminaison d'un VPC, consultez Contrôle de l'accès aux services avec des points de terminaison d'un VPC dans le guide de l'utilisateur VPC.

Supprimer l'accès à un point d'accès multi-Régions à partir d'un point de terminaison d'un VPC

Si vous possédez un point d'accès multi-régions et souhaitez en supprimer l'accès à partir d'un point de terminaison d'interface, vous devrez fournir une nouvelle stratégie d'accès au point d'accès multi-régions qui empêche l'accès aux demandes provenant des points de terminaison d'un VPC. Cependant, si les compartiments de votre point d'accès multi-régions prennent en charge les demandes via des points de terminaison d'un VPC, ils continueront à prendre en charge ces demandes. Si vous souhaitez empêcher cette prise en charge, vous devrez également mettre à jour les politiques des compartiments. La fourniture d'une nouvelle stratégie d'accès au point d'accès multi-régions empêche uniquement l'accès au point d'accès multi-régions, pas aux compartiments sous-jacents.

> **Note**
>
> Vous ne pouvez pas supprimer une politique d'accès pour un point d'accès multi-Régions. Pour supprimer l'accès à un point d'accès multi-Régions, vous devez fournir une nouvelle politique d'accès avec l'accès modifié souhaité.

Au lieu de mettre à jour la stratégie d'accès pour le point d'accès multi-régions, vous pouvez mettre à jour les politiques de compartiment pour empêcher les demandes via les points de terminaison d'un VPC. Dans ce cas, les utilisateurs peuvent toujours accéder au point d'accès multi-régions via le point de terminaison d'un VPC. Mais si la demande de point d'accès multi-régions est acheminée vers un compartiment où la politique de compartiment empêche l'accès, elle générera un message d'erreur.

Effectuer des requêtes par l'intermédiaire d'un point d'accès multi-régions

Comme les autres ressources, les points d'accès multirégionaux Amazon S3 ont des noms de ressources Amazon (ARNs). Vous pouvez les utiliser ARNs pour diriger les demandes vers des points d'accès multirégionaux à l'aide de AWS Command Line Interface (AWS CLI) ou de l'API Amazon S3. AWS SDKs Vous pouvez également les utiliser ARNs pour identifier les points d'accès multirégionaux dans les politiques de contrôle d'accès. Un ARN de point d'accès multi-régions n'inclut pas ou ne divulgue pas son nom. Pour plus d'informations sur ARNs, consultez Amazon Resource Names (ARNs) dans le Références générales AWS.

> **Note**
>
> L'alias et l'ARN du point d'accès multirégion ne peuvent pas être utilisés de manière interchangeable.

Le point d'accès multirégional ARNs utilise le format suivant :

`arn:aws:s3::`*`account-id`*`:accesspoint/`*`MultiRegionAccessPoint_alias`*

Voici quelques exemples de points ARNs d'accès multirégionaux :

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap`représente le point d'accès multirégional avec l'alias`mfzwi23gnjvgw.mrap`, qui appartient à Compte AWS `123456789012`.
- `arn:aws:s3::123456789012:accesspoint/*` représente tous les points d'accès multi-régions du compte `123456789012`. Cet ARN correspond à tous les points d'accès multi-régions du compte `123456789012`, mais il ne correspond à aucun point d'accès Amazon S3 régional, car l'ARN n'inclut pas de Région AWS. En revanche, l'ARN `arn:aws:s3:us-west-2:123456789012:accesspoint/*` correspond à tous les points d'accès Amazon S3 régionaux de la région `us-west-2` pour le compte `123456789012`, mais il ne correspond à aucun point d'accès multi-régions.

ARNs pour les objets accessibles via un point d'accès multirégional, utilisez le format suivant :

`arn:aws:s3::`*`account_id`*`:accesspoint/`*`MultiRegionAccessPoint_alias`*`//`*`key`*

Comme pour les points d'accès multirégionaux ARNs, ARNs les objets accessibles via des points d'accès multirégionaux n'incluent pas de. Région AWS Voici quelques exemples.

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01` représente l'objet `-01`, accessible via le point d'accès multi-régions avec l'alias `mfzwi23gnjvgw.mrap`, qui appartient à un compte `123456789012`.
- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//*` représente tous les objets accessibles via le point d'accès multi-régions avec l'alias `mfzwi23gnjvgw.mrap`, dans un compte `123456789012`.

- `arn:aws:s3::123456789012:accesspoint/mfzwi23gnjvgw.mrap//-01/finance/*` représente tous les objets accessibles sous le préfixe `-01/finance/` pour le point d'accès multi-régions avec l'alias `mfzwi23gnjvgw.mrap`, dans un compte `123456789012`.

Noms d'hôte des points d'accès multi-Régions

Vous pouvez accéder aux données Amazon S3 via un point d'accès multi-régions à l'aide du nom d'hôte du point d'accès multi-régions. Les requêtes peuvent être dirigées vers ce nom d'hôte depuis l'Internet public. Si vous avez configuré une ou plusieurs passerelles Internet pour le point d'accès multi-régions, les requêtes peuvent également être dirigées vers ce nom d'hôte depuis un cloud privé virtuel (VPC). Pour en savoir plus sur la création de points de terminaison d'interface VPC à utiliser avec des points d'accès multi-Régions, consultez Configurer un point d'accès multi-Régions pour utilisation avec AWS PrivateLink.

Pour effectuer des demandes via un point d'accès multi-régions à partir d'un VPC utilisant un point de terminaison d'un VPC, vous pouvez utiliser AWS PrivateLink. Lorsque vous envoyez des demandes à un point d'accès multirégional en utilisant AWS PrivateLink, vous ne pouvez pas utiliser directement un nom DNS (Regional DOMAIN NAME SYSTEM) spécifique au point de terminaison qui se termine par. *`region`*`.vpce.amazonaws.com` Ce nom d'hôte ne sera pas associé à un certificat, il ne peut donc pas être utilisé directement. Vous pouvez toujours utiliser le nom de système de nom de domaine (DNS) public du point de terminaison d'un VPC comme une cible `CNAME` ou `ALIAS`. Vous pouvez également activer le système de nom de domaine (DNS) privé sur le point de terminaison et utiliser le nom du système de nom de domaine (DNS) standard *`MultiRegionAccessPoint_alias`*`.accesspoint.s3-global.amazonaws.com` du point d'accès multi-régions, comme décrit dans cette section.

Lorsque vous faites des demandes à l'API pour les opérations sur les données Amazon S3 (par exemple, `GetObject`) via un point d'accès multi-régions, le nom d'hôte de la demande est le suivant :

`MultiRegionAccessPoint_alias``.accesspoint.s3-global.amazonaws.com`

Par exemple, pour effectuer une requête `GetObject` via le point d'accès multi-régions avec l'alias `mfzwi23gnjvgw.mrap`, faites une demande au nom d'hôte `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`. La partie `s3-global` du nom d'hôte indique que ce nom d'hôte n'est pas destiné à une région particulière.

Faire des demandes via un point d'accès multi-Régions est similaire à faire des demandes via un point d'accès à une seule Région. Toutefois, il est important de connaître les différences suivantes :

- Le point d'accès multirégional ARNs n'inclut pas de Région AWS. Ils suivent le format `arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias`.
- Pour les demandes effectuées via des opérations d'API (ces demandes ne nécessitent pas l'utilisation d'un ARN), les points d'accès multi-régions utilisent un modèle de point de terminaison différent. Le est est `MultiRegionAccessPoint_alias.accesspoint.s3-global.amazonaws.com` (par exemple, `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`). Notez les différences par rapport à un point d'accès à une seule Région :
  - Les noms d'hôtes de points d'accès multi-Régions utilisent leurs alias, pas le nom du point d'accès multi-Régions.
  - Les noms d'hôte des points d'accès multirégionaux n'incluent pas l'identifiant du Compte AWS propriétaire.
  - Les noms d'hôtes des points d'accès multi-régions n'incluent aucune Région AWS.
  - Les noms d'hôte des points d'accès multi-Régions incluent `s3-global.amazonaws.com` au lieu de `s3.amazonaws.com`.
- Les requêtes de points d'accès multi-régions doivent être signées en utilisant la version 4A de la signature (SigV4A). Lorsque vous utilisez le AWS SDKs, le SDK convertit automatiquement un SigV4 en SigV4a. Par conséquent, vérifiez que votre version de votre kit SDK AWS prend en charge SigV4A comme mise en œuvre de la signature qui est utilisée pour signer les demandes pour les Région AWS mondiales. Pour plus d'informations sur SIGv4a, consultez la section Signature des demandes AWS d'API dans le. Références générales AWS

Points d'accès multi-Régions et Amazon S3 Transfer Acceleration

Amazon S3 Transfer Acceleration est une fonction qui permet des transferts de données rapides vers des compartiments. L'accélération du transfert est configurée au niveau de chaque compartiment. Pour plus d'informations sur Transfer Acceleration, consultez Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.

Les points d'accès multirégionaux utilisent un mécanisme de transfert accéléré similaire à celui de l'accélération du transfert pour envoyer des objets volumineux sur le AWS réseau. Pour cette raison, vous n'avez pas besoin d'utiliser l'accélération du transfert lorsque vous envoyez des requêtes via un point d'accès multi-régions. Ces performances de transfert accrues sont automatiquement intégrées au point d'accès multi-régions.

Rubriques

- Autorisations
- Restrictions et limitations des points d'accès multi-régions
- Routage des demandes de points d'accès multi-Régions
- Contrôles de basculement des points d'accès multi-régions Amazon S3
- Configuration de la réplication à utiliser avec des points d'accès multi-régions
- Utilisation de points d'accès multi-régions avec des opérations d'API prises en charge
- Surveillance et journalisation des demandes effectuées via un point d'accès multi-Régions vers les ressources sous-jacentes

Autorisations

Les points d'accès multirégionaux Amazon S3 peuvent simplifier l'accès aux données pour plusieurs compartiments Amazon S3. Régions AWS Les points d'accès multi-régions sont des points de terminaison mondiaux nommés que vous pouvez utiliser pour effectuer des opérations sur les objets d'accès aux données Amazon S3, telles que `GetObject` et `PutObject`. Chaque point d'accès multi-régions peut comporter des autorisations et des contrôles de réseau distincts pour toute requête effectuée par le point de terminaison global.

Chaque point d'accès multi-régions peut également appliquer une stratégie d'accès personnalisée qui fonctionne conjointement avec la politique de compartiment attachée au compartiment sous-jacent. Pour qu'une demande entre comptes aboutisse, les règles suivantes doivent autoriser l'opération :

- La politique de point d'accès multi-régions
- La politique sous-jacente AWS Identity and Access Management (IAM)
- La politique de compartiment sous-jacente (vers laquelle la requête est routée).

> **Note**
>
> Pour les demandes portant sur le même compte, seule la politique IAM sous-jacente, qui accorde l'accès approprié, est requise.

Vous pouvez configurer toute politique de point d'accès multi-régions pour qu'elle n'accepte que les requêtes provenant d'utilisateurs ou de groupes IAM spécifiques. Pour obtenir un exemple de la manière de procéder, consultez l'exemple 2 dans the section called "Exemples de politique de

point d'accès multi-régions". Pour limiter l'accès aux données Amazon S3 à un réseau privé, vous pouvez configurer la politique de point d'accès multi-régions pour accepter les requêtes provenant uniquement d'un cloud privé virtuel (VPC).

Supposons, par exemple, que vous fassiez une `GetObject` demande via un point d'accès multirégional en utilisant un utilisateur appelé `AppDataReader` dans votre AWS compte. Pour vous assurer que la demande ne sera pas refusée, l'utilisateur `AppDataReader` doit se voir accorder l'autorisation `s3:GetObject` par le point d'accès multi-Régions et par chaque compartiment sous-jacent au point d'accès multi-Régions. `AppDataReader` ne sera pas en mesure de récupérer des données d'un compartiment qui n'octroie pas cette autorisation.

> **Important**
>
> La délégation du contrôle d'accès d'un compartiment à une politique de point d'accès multi-régions ne modifie pas le comportement du compartiment lorsqu'on y accède directement par son nom de compartiment ou Amazon Resource Name (ARN). Toutes les opérations effectuées directement sur le compartiment continueront à fonctionner comme avant. Les restrictions que vous incluez dans une politique de point d'accès multi-régions s'appliquent uniquement aux demandes effectuées via ce point d'accès.

Gestion de l'accès public vers un point d'accès multi-Régions

Les points d'accès multi-Régions prennent en charge des paramètres de blocage d'accès public indépendants pour chaque point d'accès multi-Régions. Lorsque vous créez un point d'accès multi-Régions, vous pouvez indiquer les paramètres de blocage d'accès public qui s'appliquent à ce point d'accès multi-Régions.

> **Note**
>
> Tous les paramètres de blocage de l'accès public qui sont activés dans Paramètres de blocage de l'accès public pour ce compte (dans votre propre compte) ou dans Paramètres de blocage public pour les compartiments externes s'appliquent, même si les paramètres indépendants de blocage de l'accès public pour votre point d'accès multi-régions sont désactivés.

Pour toute requête effectuée par le biais d'un point d'accès multi-régions, Amazon S3 évalue les paramètres de blocage de l'accès public pour les éléments suivants :

- Le point d'accès multi-régions
- Les compartiments sous-jacents (y compris les compartiments externes)
- Le compte propriétaire du point d'accès multi-régions
- Le compte propriétaire des compartiments sous-jacents (y compris les comptes externes)

Si l'un de ces paramètres indique que la demande doit être bloquée, Amazon S3 rejettera la demande. Pour en savoir de plus sur le blocage de l'accès public Amazon S3, consultez Blocage de l'accès public à votre stockage Amazon S3.

> **Important**
>
> Tous les paramètres de blocage de l'accès public sont activés par défaut pour les points d'accès. Vous devez désactiver explicitement tous les paramètres que vous ne souhaitez pas appliquer à un point d'accès multi-Régions.
> Vous ne pouvez pas modifier les paramètres de blocage de l'accès public après la création du point d'accès multi-régions.

Affichage des paramètres de blocage d'accès public pour un point d'accès multi-régions

Pour afficher les paramètres de blocage d'accès public d'un point d'accès multi-régions, procédez comme suit

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Choisissez le nom du point d'accès multi-régions que vous voulez examiner.
4. Sélectionnez l'onglet Autorisations.
5. Sous Block Public Access settings for this Multi-Region Access Point (Bloquer les paramètres d'accès public pour ce point d'accès multi-régions), vérifiez les paramètres de blocage de l'accès public pour votre point d'accès multi-régions.

> **Note**
>
> Vous ne pouvez pas modifier les paramètres de blocage de l'accès public après la création du point d'accès multi-régions. Par conséquent, si vous avez l'intention de bloquer l'accès public, assurez-vous que vos applications fonctionnent correctement sans accès public avant de créer un point d'accès multi-régions.

Utilisation d'une politique de point d'accès multi-régions

L'exemple suivant de politique de point d'accès multi-régions accorde à un utilisateur IAM l'accès à la liste et au téléchargement de fichiers depuis votre point d'accès multi-régions. Pour utiliser cet exemple de politique, remplacez *user input placeholders* par vos propres informations.

JSON

```
 {
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "AWS":"arn:aws:iam::123456789012:user/JohnDoe"
         },
         "Action":[
            "s3:ListBucket",
            "s3:GetObject"
         ],
         "Resource":[
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
            "arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/
object/*"
         ]
      }
   ]
}
```

Pour associer votre politique de point d'accès multi-régions au point d'accès multi-régions spécifié avec AWS Command Line Interface (AWS CLI), utilisez la commande `put-multi-region-`

`access-point-policy` suivante. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations. Chaque point d'accès multi-régions ne peut avoir qu'une seule politique, donc une demande faite à l'action `put-multi-region-access-point-policy` remplace toute politique existante associée au point d'accès multi-régions spécifié.

AWS CLI

```
aws s3control put-multi-region-access-point-policy
--account-id 111122223333
--details { "Name": "amzn-s3-demo-bucket-MultiRegionAccessPoint",
 "Policy": "{ \"Version\": \"2012-10-17\", \"Statement\": { \"Effect\":
 \"Allow\", \"Principal\": { \"AWS\": \"arn:aws:iam::111122223333:root
\" }, \"Action\": [\"s3:ListBucket\", \"s3:GetObject\"], \"Resource\":
 [ \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias",
 \"arn:aws:s3::111122223333:accesspoint/MultiRegionAccessPoint_alias/object/*
\" ] } }" }
```

Pour interroger les résultats de l'opération précédente, utilisez la commande suivante :

AWS CLI

```
aws s3control describe-multi-region-access-point-operation
--account-id 111122223333
--request-token-arn requestArn
```

Pour récupérer votre politique de point d'accès multi-régions, utilisez la commande suivante :

AWS CLI

```
aws s3control get-multi-region-access-point-policy
--account-id 111122223333
--name=amzn-s3-demo-bucket-MultiRegionAccessPoint
```

Modification de la politique de point d'accès multi-régions

La politique de point d'accès multi-régions (écrite en JSON) fournit un accès de stockage aux compartiments Amazon S3 qui sont utilisés avec ce point d'accès multi-régions. Vous pouvez autoriser ou empêcher des principaux spécifiques d'effectuer diverses actions sur votre point d'accès

multi-régions. Lorsqu'une requête est routée vers un compartiment via le point d'accès multi-régions, les stratégies d'accès du point d'accès multi-régions et du compartiment s'appliquent. La stratégie d'accès la plus restrictive a toujours la priorité.

> **Note**
>
> Si un compartiment contient des objets appartenant à d'autres comptes, la politique du point d'accès multi-régions ne s'applique pas aux objets appartenant à d'autres Comptes AWS.

Après avoir appliqué une politique de point d'accès multi-régions, la politique ne peut pas être supprimée. Vous pouvez soit modifier la politique, soit créer une nouvelle politique qui écrase la politique existante.

Pour modifier la politique de point d'accès multi-régions

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Choisissez le nom du point d'accès multi-régions pour lequel vous souhaitez modifier la politique.
4. Sélectionnez l'onglet Autorisations.
5. Faites défiler vers le bas jusqu'à la section Multi-Region Access Point policy (Politique de point d'accès multi-régions). Choisissez Edit (Modifier) pour mettre à jour la politique (en JSON).
6. La page Edit Multi-Region Access Point policy (Modifier la politique de point d'accès multi-régions) s'affiche. Vous pouvez soit saisir la politique directement dans le champ de texte, soit choisir Add statement (Ajouter une instruction) pour sélectionner les éléments de la politique dans une liste déroulante.

   > **Note**
   >
   > La console affiche automatiquement l'Amazon Resource Name (ARN) du point d'accès multi-régions, que vous pouvez utiliser dans la politique. Pour obtenir des exemples de politique de point d'accès multi-régions, consultez the section called "Exemples de politique de point d'accès multi-régions".

Exemples de politique de point d'accès multi-régions

Politiques de ressources de prise en charge AWS Identity and Access Management (IAM) des points d'accès multirégionaux Amazon S3. Ces politiques peuvent contrôler l'utilisation du point d'accès multi-régions par ressource, par utilisateur ou d'autres conditions. Pour qu'une application ou un utilisateur puisse accéder à des objets par le biais d'un point d'accès multi-régions, le point d'accès multi-régions et le compartiment sous-jacent doivent tous deux permettre le même accès.

Pour autoriser le même accès à la fois au point d'accès multi-régions et au compartiment sous-jacent, effectuez l'une des opérations suivantes :

- (Recommandé) Pour simplifier les contrôles d'accès lors de l'utilisation d'un point d'accès multi-régions Amazon S3, déléguez le contrôle d'accès pour le compartiment Amazon S3 au point d'accès multi-régions. Pour obtenir un exemple de la manière de procéder, reportez-vous à l'exemple 1 de cette section.
- Ajoutez les mêmes autorisations contenues dans la politique de point d'accès multi-régions à la politique de compartiment sous-jacente.

> **Important**
>
> La délégation du contrôle d'accès d'un compartiment à une politique de point d'accès multi-régions ne modifie pas le comportement du compartiment lorsqu'on y accède directement par son nom de compartiment ou Amazon Resource Name (ARN). Toutes les opérations effectuées directement sur le compartiment continueront à fonctionner comme avant. Les restrictions que vous incluez dans une politique de point d'accès multi-régions s'appliquent uniquement aux demandes effectuées via ce point d'accès.

Example 1 : délégation de l'accès à des points d'accès multi-régions spécifiques dans votre politique de compartiment (pour le même compte ou intercompte)

L'exemple suivant de politique de compartiment permet un accès complet à un point d'accès multi-régions spécifique. Cela signifie que tout accès à ce compartiment est contrôlé par les politiques qui sont attachées au point d'accès multi-régions. Nous vous recommandons de configurer vos compartiments de cette façon pour tous les cas d'utilisation qui ne demandent pas d'accès direct au compartiment. Vous pouvez utiliser cette structure de politique de compartiment pour les points d'accès multi-régions du même compte ou d'un autre compte.

JSON

```
{
    "Version": "2012-10-17",
    "Statement" : [
    {
        "Effect": "Allow",
        "Principal" : { "AWS": "*" },
        "Action" : "*",
        "Resource" : [ "arn:aws:s3:::amzn-s3-demo-bucket", "arn:aws:s3:::amzn-s3-
demo-bucket/*"],
        "Condition": {
            "StringEquals" : { "s3:DataAccessPointArn" :
 "arn:aws:s3::111122223333:accesspoint/example-multi-region-access-point" }
        }
    }]
}
```

> **Note**
>
> Si vous accordez l'accès à plusieurs points d'accès multi-régions, assurez-vous de lister chaque point d'accès multi-régions.

Example 2 : accorder l'accès d'un compte à un point d'accès multi-régions dans votre politique de point d'accès multi-régions

La stratégie de point d'accès multi-région suivante accorde l'autorisation au compte *123456789012* de lister et de lire les objets contenus dans le point d'accès multi-région défini par *MultiRegionAccessPoint_ARN*.

JSON

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

```
            "AWS":"arn:aws:iam::111122223333:user/JohnDoe"
         },
         "Action":[
            "s3:ListBucket",
            "s3:GetObject"
         ],
         "Resource":[
            "MultiRegionAccessPoint_ARN",
            "MultiRegionAccessPoint_ARN/object/*"
         ]
      }
   ]
}
```

Example 3 – Stratégie de point d'accès multi-région autorisant le listage des compartiments

La stratégie de point d'accès multi-région suivante accorde l'autorisation au compte *123456789012* de lister les objets contenus dans le point d'accès multi-région défini par *MultiRegionAccessPoint_ARN*.

JSON

```
{
   "Version":"2012-10-17",
   "Statement": [
      {
       "Effect": "Allow",
       "Principal": {
        "AWS": "arn:aws:iam::111122223333:user/JohnDoe"
        },
        "Action": "s3:ListBucket",
        "Resource": "MultiRegionAccessPoint_ARN"
       }
    ]
}
```

Restrictions et limitations des points d'accès multi-régions

Les points d'accès Amazon S3 comportent les restrictions et limitations suivantes :

Noms et alias

Les noms de points d'accès multirégionaux doivent répondre aux exigences suivantes :

- Doit être unique au sein d'un seul AWS compte.
- Ils doivent commencer par un chiffre ou une lettre minuscule.
- Ils doivent comporter entre 3 et 50 caractères.
- Impossible de commencer ou de terminer par un tiret (`-`).
- Ne peut pas contenir de traits de soulignement (`_`), de lettres majuscules ou de points (`.`).
- Il est impossible de les modifier après qu'ils aient été créés.

Les alias de point d'accès multirégional (qui sont différents du nom d'un point d'accès multirégional) sont générés automatiquement par Amazon S3 et ne peuvent être ni modifiés ni réutilisés. Pour plus d'informations sur la différence entre les alias de point d'accès multirégionaux et les noms de points d'accès multirégionaux et sur leurs règles de dénomination respectives, consultez. Règles relatives à l'attribution de noms pour les points d'accès multi-Régions Amazon S3

Accès à un point d'accès multirégional

Vous ne pouvez pas accéder aux données via un point d'accès multirégional en utilisant des points de terminaison de passerelle. En revanche, vous pouvez accéder aux données via un point d'accès multi-région en utilisant des points de terminaison d'interface. Pour l'utiliser AWS PrivateLink, vous devez créer des points de terminaison VPC. Pour de plus amples informations, veuillez consulter Configurer un point d'accès multi-Régions pour utilisation avec AWS PrivateLink. Cependant, sachez que cela IPv6 n'est pas pris en charge.

Pour utiliser des points d'accès multirégionaux avec Amazon CloudFront, vous devez configurer le point d'accès multirégional en tant que type de `Custom Origin` distribution. Pour plus d'informations sur les différents types d'origine, consultez la section Utilisation de différentes origines avec CloudFront les distributions. Pour plus d'informations sur l'utilisation de points d'accès multirégionaux avec Amazon CloudFront, consultez la section Création d'une application active-active basée sur la proximité dans plusieurs régions sur le blog sur le stockage.AWS

> **Note**
>
> Les buckets S3 on Outposts ne sont pas pris en charge.

Signature des demandes AWS d'API

Pour signer une demande d' AWS API, votre point d'accès multirégional doit répondre aux exigences minimales suivantes :

> **Note**
>
> Les points d'accès multi-régions ne prennent pas en charge les demandes anonymes.

- Support de la version 1.2 du protocole TLS (Transport Layer Security).
- Support pour la version 4 de signature (SigV4a) : cette version de SigV4 permet de signer des demandes pour plusieurs. Régions AWS Cette fonction est utile dans les opérations d'API qui peuvent entraîner un accès aux données à partir d'une de plusieurs régions. Lorsque vous utilisez un AWS SDK, vous fournissez vos informations d'identification, et les demandes adressées aux points d'accès multirégionaux utiliseront la version 4A de Signature sans configuration supplémentaire. Assurez-vous de vérifier la compatibilité de votre kit AWS SDK avec l'algorithme SigV4A. Pour plus d'informations sur SIGv4a, consultez la section Signature des demandes AWS d'API dans le. Références générales AWS

  > **Note**
  >
  > Pour utiliser SigV4A avec des informations d'identification de sécurité temporaires, par exemple, lorsque vous utilisez des rôles AWS Identity and Access Management (IAM), vous pouvez demander les informations d'identification temporaires à un point de terminaison régional (). AWS Security Token Service AWS STS Si vous demandez les informations d'identification temporaires à partir du point de terminaison AWS STS global (`sts.amazonaws.com`), vous devez d'abord définir la compatibilité régionale des jetons de session pour que le point de terminaison global soit valide dans toutes les Régions AWS. Pour plus d'informations, consultez la section Gestion AWS STS dans et Région AWS dans le guide de l'utilisateur IAM.

Opérations de l'API Amazon S3

- `CopyObject`est prise en charge en tant que destination uniquement lors de l'utilisation de l'ARN du point d'accès multirégional.
- La fonctionnalité S3 Batch Operations n'est pas prise en charge.

AWS SDKs

Certains AWS SDKs ne sont pas pris en charge. Pour vérifier ceux qui AWS SDKs sont pris en charge pour les points d'accès multirégionaux, consultez la section Compatibilité avec AWS SDKs.

Quotas de service

Tenez compte des limites de quotas de service suivantes :

- Il existe une limite maximale de 100 points d'accès multi-régions par compte.
- Il existe une limite de 17 régions pour un seul point d'accès multi-régions.

Création, suppression ou modification d'un point d'accès multirégional

Lorsque vous créez, supprimez ou modifiez un point d'accès multirégional, tenez compte des règles et restrictions suivantes :

- Une fois le point d'accès multi-régions créé, vous ne pouvez pas ajouter, modifier ou supprimer des compartiments de la configuration du point d'accès multi-régions. Pour modifier les compartiments, vous devrez supprimer tout le point d'accès multi-Régions et en créer un autre. Si un compartiment multi-comptes de votre point d'accès multi-régions est supprimé, la seule façon de reconnecter ce compartiment est de le recréer, en utilisant le même nom et la même région dans ce compte.
- Les compartiments sous-jacents (dans le même compte) utilisés dans un point d'accès multi-régions peuvent être supprimés uniquement si ce point d'accès multi-régions est supprimé.

Prise en charge de la région

Demandes de plan de contrôle

Toutes les demandes du plan de contrôle de création ou de gestion de points d'accès multirégions doivent être routées vers la région `US West (Oregon)`. Pour les demandes de plan de données de points d'accès multirégions, il n'est pas nécessaire de spécifier les régions.

Pour le plan de contrôle de basculement des points d'accès multirégions, les demandes doivent être routées vers l'une des cinq régions prises en charge suivantes :

- `US East (N. Virginia)`
- `US West (Oregon)`

- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Europe (Ireland)

Régions activées par défaut

Votre point d'accès multirégional prend en charge les compartiments par défaut suivants Régions AWS (qui sont activés par défaut dans votre Compte AWS) :

- US East (N. Virginia)
- US East (Ohio)
- US West (N. California)
- US West (Oregon)
- Asia Pacific (Mumbai)
- Asia Pacific (Osaka)
- Asia Pacific (Seoul)
- Asia Pacific (Singapore)
- Asia Pacific (Sydney)
- Asia Pacific (Tokyo)
- Canada (Central)
- Europe (Frankfurt)
- Europe (Ireland)
- Europe (London)
- Europe (Paris)
- Europe (Stockholm)
- South America (São Paulo)

AWS Régions optionnelles

Votre point d'accès multirégional prend également en charge les buckets dans le cadre de l'opt-in suivant Régions AWS (qui sont désactivés par défaut dans votre) : Compte AWS

- Africa (Cape Town)

- Asia Pacific (Hong Kong)
- Asia Pacific (Jakarta)
- Asia Pacific (Melbourne)
- Asia Pacific (Hyderabad)
- Canada West (Calgary)
- Europe (Zurich)
- Europe (Milan)
- Europe (Spain)
- Israel (Tel Aviv)
- Middle East (Bahrain)
- Middle East (UAE)

> **Note**
>
> L'activation d'une région optionnelle n'entraîne aucun coût supplémentaire. Cependant, la création ou l'utilisation d'une ressource dans un point d'accès multirégional entraîne des frais de facturation.

Une région optionnelle doit être activée manuellement lors de la configuration ou de la création de votre point d'accès multirégional. Pour plus d'informations sur les comportements régionaux optionnels pour les points d'accès multirégionaux, consultez. Configuration des régions optionnelles aux points d'accès multirégionaux Pour plus d'informations sur la façon d'activer une région optionnelle dans votre Compte AWS, consultez la section Activer ou désactiver une région pour les comptes autonomes dans le Guide de référence de gestion des AWS comptes.

Routage des demandes de points d'accès multi-Régions

Lorsque vous effectuez une demande via un point d'accès multi-régions, Amazon S3 détermine lequel des compartiments associés au point d'accès multi-régions est le plus proche de vous. Amazon S3 dirige ensuite la demande vers ce compartiment, quelle que soit la AWS région dans laquelle il se trouve.

Une fois que le point d'accès multi-régions a acheminé la demande vers le compartiment le plus proche, Amazon S3 traite la demande comme si vous l'aviez adressée directement à ce

compartiment. Les points d'accès multi-régions ne connaissent pas le contenu des données d'un compartiment Amazon S3. Par conséquent, le compartiment qui reçoit la demande peut ne pas contenir les données demandées. Pour créer des jeux de données cohérents dans les compartiments Amazon S3 associés à un point d'accès multi-régions, vous pouvez configurer la réplication entre régions (CRR) S3. Ensuite, n'importe quel compartiment peut répondre à la demande avec succès.

Amazon S3 dirige les demandes de points d'accès multi-Régions conformément aux règles suivantes :

- Amazon S3 optimise l'exécution des requêtes en fonction de leur proximité. Il examine les compartiments pris en charge par le point d'accès multi-régions et transmet la requête au compartiment le plus proche.
- Si la demande indique une ressource existante (par exemple, `GetObject`), Amazon S3 peut ne pas tenir compte du nom de l'objet lorsqu'il exécutera la demande. Cela signifie que même si un objet existe dans un compartiment dans le point d'accès multi-régions, votre demande peut être acheminée vers un compartiment qui ne contient pas l'objet. Cela entraînera un message d'erreur 404 retourné au client.

  Pour éviter les erreurs 404, nous vous recommandons de configurer la réplication entre régions (CRR) S3 pour vos compartiments. La réplication permet de résoudre le problème potentiel lorsque l'objet que vous voulez est dans un compartiment dans le point d'accès multi-régions, mais qu'il ne se trouve pas dans le compartiment spécifique vers lequel votre demande a été acheminée. Pour obtenir des informations sur la configuration de réplication de base, consultez Configuration de la réplication à utiliser avec des points d'accès multi-régions.

  Pour garantir que vos demandes sont satisfaites en utilisant les objets spécifiques que vous souhaitez, nous vous recommandons également d'activer le versionnement des compartiments et d'inclure la version IDs dans vos demandes. Cette approche permet de vous assurer que vous disposez de la version correcte de l'objet que vous recherchez. Les compartiments avec la gestion des versions activée vous permettent de récupérer des objets en cas de remplacement accidentel. Pour plus d'informations, consultez Utilisation de la gestion des versions dans les compartiments S3.
- Si la demande vise à créer une ressource (par exemple, `PutObject` ou `CreateMultipartUpload`), Amazon S3 répond à la demande en utilisant le compartiment le plus proche. Prenons l'exemple d'une société de vidéo qui souhaite prendre en charge les chargements de vidéos de n'importe où dans le monde vers le compartiment le plus proche. Lorsqu'un utilisateur effectue une demande PUT au point d'accès multi-régions, l'objet est placé dans le compartiment le plus proche. Pour ensuite permettre à des utilisateurs du monde entier de télécharger cette vidéo

avec la latence la plus faible, vous pouvez utiliser le CRR avec une réplication bidirectionnelle. L'utilisation du CRR avec une réplication bidirectionnelle permet de synchroniser le contenu de tous les compartiments associés au point d'accès multi-régions. Pour plus d'informations sur la réplication avec des points d'accès multi-régions, consultez Configuration de la réplication à utiliser avec des points d'accès multi-régions.

Contrôles de basculement des points d'accès multi-régions Amazon S3

Grâce aux contrôles de basculement du point d'accès multi-régions d'Amazon S3, vous pouvez maintenir la continuité des activités pendant les perturbations du trafic régional, tout en offrant à vos applications une architecture multi-régions pour répondre aux besoins de conformité et de redondance. Si votre trafic régional est perturbé, vous pouvez utiliser les contrôles de basculement des points d'accès multirégionaux pour sélectionner celui situé Régions AWS derrière un point d'accès multirégional Amazon S3 qui traitera les demandes d'accès aux données et de stockage.

Pour prendre en charge le basculement, vous pouvez configurer votre point d'accès multi-régions dans une configuration active-passive, le trafic circulant vers la région active dans des conditions normales, et une région passive de secours pour le basculement.

Par exemple, pour effectuer un basculement vers une région Région AWS de votre choix, vous devez transférer le trafic de votre région principale (active) vers votre région secondaire (passive). Dans une configuration active-passive comme celle-ci, un compartiment est actif et accepte le trafic, tandis que l'autre est passif et n'accepte pas le trafic. Le compartiment passif est utilisé pour la reprise après sinistre. Lorsque vous lancez le basculement, tout le trafic (tel que les requêtes `GET` et `PUT`) est dirigé vers le compartiment actif (dans une région) et éloigné du compartiment passif (dans une autre région).

Si vous avez activé la réplication entre régions (CRR) de S3 avec des règles de réplication bidirectionnelle, vous pouvez garder vos compartiments synchronisés pendant un basculement. En outre, si vous avez activé la fonction CRR dans une configuration active-active, les points d'accès multi-régions d'Amazon S3 peuvent également récupérer des données à partir de l'emplacement du compartiment le plus proche, ce qui améliore les performances des applications.

Région AWS soutien

Grâce aux contrôles de basculement des points d'accès multi-régions d'Amazon S3, vos compartiments S3 peuvent se trouver dans l'une des 17 régions où les points d'accès multi-régions sont pris en charge. Vous pouvez initier un basculement sur deux régions à la fois.

> **Note**
>
> Bien que le basculement ne soit initié qu'entre deux régions à la fois, vous pouvez mettre à jour séparément les statuts de routage pour plusieurs régions en même temps dans votre point d'accès multi-régions.

Les rubriques suivantes expliquent comment utiliser et gérer les contrôles de basculement du point d'accès multi-régions Amazon S3.

Rubriques

- États d'acheminement des points d'accès multi-régions Amazon S3
- Utilisation des contrôles de basculement du point d'accès multi-régions d'Amazon S3
- Erreurs de contrôle du basculement du point d'accès multi-régions Amazon S3

États d'acheminement des points d'accès multi-régions Amazon S3

Votre configuration de basculement des points d'accès multi-régions Amazon S3 détermine le statut de routage de la Régions AWS utilisée avec le point d'accès multi-régions. Vous pouvez configurer votre point d'accès multi-régions Amazon S3 pour qu'il soit dans un état actif-actif ou actif-passif.

- Active-active : dans une configuration active-active, toutes les requêtes sont automatiquement envoyées vers la Région AWS la plus proche de votre point d'accès multi-régions. Une fois que le point d'accès multi-régions a été configuré pour être dans un état actif-actif, toutes les régions peuvent recevoir du trafic. Si une interruption du trafic se produit dans une configuration active-active, le trafic réseau sera automatiquement redirigé vers l'une des régions actives.
- Active-passive : dans une configuration active-passive, les régions actives de votre point d'accès multi-régions reçoivent du trafic et les régions passives n'en reçoivent pas. Si vous avez l'intention d'utiliser les contrôles de basculement S3 pour initier le basculement en cas de sinistre, configurez vos points d'accès multi-régions dans une configuration active-passive pendant les tests et la planification de la reprise après sinistre.

Utilisation des contrôles de basculement du point d'accès multi-régions d'Amazon S3

Cette section explique comment gérer et utiliser les contrôles de basculement de vos points d'accès multi-régions Amazon S3 à l'aide de la fonction AWS Management Console.

Il existe deux contrôles de basculement dans la section Configuration du basculement de la page de détails de votre point d'accès multirégional, dans les rubriques AWS Management Console : Modifier le statut du routage et Basculement. Vous pouvez utiliser ces contrôles comme suit :

- Modifier l'état du routage — Vous pouvez modifier manuellement les états de routage d'un maximum de 17 Régions AWS en une seule demande pour votre point d'accès multirégional en choisissant Modifier le statut de routage. Vous pouvez utiliser la fonction Edit routing status (Modifier le statut de routage) pour les raisons suivantes :
  - Pour définir ou modifier les statuts d'acheminement d'une ou plusieurs régions dans votre point d'accès multi-régions.
  - Pour créer une configuration de basculement pour votre point d'accès multi-régions en configurant deux régions dans un état actif-passif.
  - Pour basculer manuellement sur vos régions
  - Pour basculer manuellement le trafic entre les régions
- Failover (Basculement): lorsque vous lancez le basculement en sélectionnant Failover (Basculement), vous ne faites que mettre à jour les statuts d'acheminement de deux régions qui sont déjà configurées pour être dans un état actif-passif. Lors d'un basculement que vous avez déclenché en sélectionnant Failover (Basculement), les statuts d'acheminement entre les deux régions sont automatiquement permutés.

Modification du statut de routage des régions dans votre point d'accès multi-régions.

Vous pouvez mettre à jour manuellement les états de routage jusqu'à 17 Régions AWS en une seule demande pour votre point d'accès multirégional en choisissant Modifier le statut de routage dans la section Configuration du basculement sur la page de détails de votre point d'accès multirégional. Cependant, lorsque vous lancez le basculement en sélectionnant Failover (Basculement), vous ne faites que mettre à jour les statuts de routage de deux régions qui sont déjà configurées pour être dans un état actif-passif. Lors d'un basculement que vous avez déclenché en sélectionnant Failover (Basculement), les statuts d'acheminement entre les deux régions sont automatiquement permutés.

Vous pouvez utiliser l'option Edit routing status (Modifier le statut de routage) comme décrit dans la procédure suivante, aux fins suivantes :

- Pour définir ou modifier les statuts d'acheminement d'une ou plusieurs régions dans votre point d'accès multi-régions.
- Pour créer une configuration de basculement pour votre point d'accès multi-régions en configurant deux régions dans un état actif-passif.

- Pour basculer manuellement sur vos régions
- Pour basculer manuellement le trafic entre les régions

Utilisation de la console S3

Pour mettre à jour le statut de routage des régions dans votre point d'accès multi-régions

1. Connectez-vous à la console AWS de gestion.
2. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
3. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
4. Choisissez le point d'accès multi-régions que vous souhaitez mettre à jour.
5. Choisissez l'onglet Replication and failover (Réplication et basculement).
6. Sélectionnez une ou plusieurs régions dont vous voulez modifier le statut de routage.

   > **Note**
   >
   > Pour initier le basculement, au moins une région Région AWS doit être désignée comme active et une région doit être désignée comme passive dans votre point d'accès multirégional.

7. Choisissez Edit routing status (Modifier le statut du routage).
8. Dans la boîte de dialogue qui s'affiche, sélectionnez Active ou Passive pour le Routing status (Statut de routage) de chaque région.

   Un état actif permet de router le trafic vers la région. Un état passif empêche tout trafic d'être dirigé vers la région.

   Si vous créez une configuration de basculement pour votre point d'accès multirégional ou si vous initiez un basculement, au moins une région Région AWS doit être désignée comme active et une région doit être désignée comme passive dans votre point d'accès multirégional.
9. Sélectionnez Save routing status (Enregistrer le statut de routage). Il faut environ deux minutes pour que le trafic soit redirigé.

Après avoir soumis le statut de routage de votre point Régions AWS d'accès multirégional, vous pouvez vérifier les modifications apportées à votre statut de routage. Pour vérifier ces modifications, rendez-vous sur Amazon CloudWatch à l'adresse suivante https://console.aws.amazon.com/cloudwatch/pour surveiller le transfert de votre trafic de demandes de données Amazon S3 (par exemple, GET et les PUT demandes) entre les régions actives et passives. Les connexions existantes ne seront pas interrompues pendant le basculement. Les connexions existantes se poursuivront jusqu'à ce qu'elles atteignent un statut de réussite ou d'échec.

À l'aide du AWS CLI

> **Note**
>
> Vous pouvez exécuter des commandes de AWS CLI routage de points d'accès multirégionaux sur l'une des cinq régions suivantes :
>
> - `ap-southeast-2`
> - `ap-northeast-1`
> - `us-east-1`
> - `us-west-2`
> - `eu-west-1`

L'exemple de commande suivant met à jour la configuration des itinéraires de votre point d'accès multi-régions actuel. Pour mettre à jour l'état actif ou passif d'un compartiment, définissez la valeur `TrafficDialPercentage` sur `100` pour actif et sur `0` pour passif. Dans cet exemple, la valeur *`amzn-s3-demo-bucket1`* est réglée sur actif, et *`amzn-s3-demo-bucket2`* est réglée sur passif. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2
,TrafficDialPercentage=0
```

L'exemple de commande suivant permet d'obtenir votre configuration de routage de point d'accès multi-régions mise à jour. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

Initialisation du basculement

Lorsque vous lancez le basculement en sélectionnant Failover (Basculement) dans la section Failover configuration (Configuration du basculement) sur la page de détails de votre point d'accès multi-régions, le trafic des demandes Amazon S3 est automatiquement transféré vers une autre Région AWS. Le processus de basculement s'achève dans les deux minutes.

Vous pouvez lancer un basculement sur deux régions Régions AWS à la fois (sur les 17 régions où les points d'accès multirégionaux sont pris en charge). Les événements de basculement sont ensuite consignés dans AWS CloudTrail. Une fois le basculement terminé, vous pouvez surveiller le trafic Amazon S3 et toutes les mises à jour du routage du trafic vers la nouvelle région active d'Amazon CloudWatch.

> **Important**
>
> Pour que toutes les métadonnées et tous les objets soient synchronisés entre les compartiments pendant la réplication des données, nous vous recommandons de créer des règles de réplication bidirectionnelle et d'activer la synchronisation des modifications des réplicas avant de configurer vos contrôles de basculement.
> Les règles de réplication bidirectionnelle permettent de s'assurer que lorsque des données sont écrites dans le compartiment Amazon S3 vers lequel le trafic bascule, ces données sont ensuite répliquées vers le compartiment source. La synchronisation des modifications des réplicas permet de s'assurer que les métadonnées des objets sont également synchronisées entre les compartiments pendant la réplication bidirectionnelle.
> Pour plus d'informations sur la configuration de la réplication pour prendre en charge le basculement, consultez the section called “Réplication de compartiment”.

Pour initier le basculement entre les compartiments répliqués

1. Connectez-vous à la console AWS de gestion.
2. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
3. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
4. Choisissez le point d'accès multi-régions que vous voulez utiliser pour initier le basculement.
5. Choisissez l'onglet Replication and failover (Réplication et basculement).
6. Descendez jusqu'à la section Failover configuration (Configuration du basculement) et sélectionnez deux Régions AWS.

   > **Note**
   >
   > Pour initier le basculement, au moins une région Région AWS doit être désignée comme active et une région doit être désignée comme passive dans votre point d'accès multirégional. Un état actif permet de diriger le trafic vers une région. Un état passif empêche tout trafic d'être dirigé vers la région.

7. Choisissez Basculement.
8. Dans la boîte de dialogue, sélectionnez Failover (Basculement) à nouveau pour lancer le processus de basculement. Au cours de ce processus, les statuts de routage des deux régions sont automatiquement permutés. Tout nouveau trafic est dirigé vers la région qui devient active, et le trafic cesse d'être dirigé vers la région qui devient passive. Il faut environ deux minutes pour que le trafic soit redirigé.

   Après avoir lancé le processus de basculement, vous pouvez contrôler vos modifications de trafic. Pour vérifier ces modifications, rendez-vous sur Amazon CloudWatch à l'adresse suivante https://console.aws.amazon.com/cloudwatch/pour surveiller le transfert de votre trafic de demandes de données Amazon S3 (par exemple, `GET` et les `PUT` demandes) entre les régions actives et passives. Les connexions existantes ne seront pas interrompues pendant le basculement. Les connexions existantes se poursuivront jusqu'à ce qu'elles atteignent un statut de réussite ou d'échec.

Visualisation des contrôles de routage de votre point d'accès multi-régions Amazon S3

Utilisation de la console S3

Pour afficher les commandes de routage de votre point d'accès Multi-Régions Amazon S3

1. Connectez-vous à la console AWS de gestion.
2. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
3. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
4. Choisissez le point d'accès multi-régions que vous voulez examiner.
5. Choisissez l'onglet Replication and failover (Réplication et basculement). Cette page affiche les détails et la synthèse de la configuration du routage pour votre point d'accès multi-régions, les règles de réplication associées et les métriques de réplication. Vous pouvez voir le statut de routage de vos régions dans la section Failover configuration (Configuration du basculement).

À l'aide du AWS CLI

L'exemple de AWS CLI commande suivant permet d'obtenir la configuration actuelle de votre itinéraire de point d'accès multirégional pour la région spécifiée. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 123456789012
--mrap MultiRegionAccessPoint_ARN
```

> **Note**
>
> Cette commande ne peut être exécutée que sur les cinq régions suivantes :
>
> - ap-southeast-2
> - ap-northeast-1
> - us-east-1
> - us-west-2
> - eu-west-1

Erreurs de contrôle du basculement du point d'accès multi-régions Amazon S3

Lorsque vous mettez à jour la configuration du basculement pour votre point d'accès multi-régions, vous pouvez rencontrer l'une des erreurs suivantes :

- HTTP 400 Demande erronée : ce problème peut survenir si vous entrez un ARN de point d'accès multi-régions non valide lors de la mise à jour de votre configuration de basculement. Vous pouvez confirmer votre ARN de point d'accès multi-régions en consultant votre politique de point d'accès multi-régions. Pour réviser ou mettre à jour votre politique de point d'accès multi-régions, consultez Editing the Multi-Region Access Point policy (Modification de la politique de point d'accès multi-régions). Cette erreur peut également se produire si vous utilisez une chaîne vide ou une chaîne aléatoire lors de la mise à jour de vos contrôles de basculement du point d'accès multi-régions Amazon S3. Veillez à utiliser le format ARN du point d'accès multi-régions :

  `arn:aws:s3::account-id:accesspoint/MultiRegionAccessPoint_alias`

- HTTP 503 Slow Down (HTTP 503 Ralentissement) : cette erreur se produit si vous envoyez trop de requêtes dans un court laps de temps. Les requêtes rejetées donneront lieu à une erreur.
- HTTP 409 Conflict (HTTP 409 Conflit) : cette erreur survient lorsque deux ou plusieurs requêtes simultanées de mise à jour de la configuration des itinéraires visent un seul point d'accès multi-régions. La première requête aboutit, mais toutes les autres échouent avec une erreur.
- Méthode HTTP 405 non autorisée : cette erreur se produit lorsque vous avez sélectionné un point d'accès multirégional avec un seul point d'accès Région AWS lors du lancement du basculement. Vous devez sélectionner deux régions avant de pouvoir lancer le basculement. Sinon, une erreur est renvoyée.

Configuration de la réplication à utiliser avec des points d'accès multi-régions

Lorsque vous adressez une demande à un point de terminaison d'accès multi-régions, Amazon S3 achemine automatiquement la demande vers le compartiment le plus proche de vous. Amazon S3 ne tient pas compte du contenu de la demande lorsqu'il prend cette décision. Si vous envoyez une demande pour `GET` un objet, votre demande peut être acheminée vers un compartiment qui n'a pas de copie de cet objet. Si c'est le cas, vous recevez un code d'erreur HTTP 404 (Not Found) [HTTP 404 (Introuvable)]. Pour plus d'informations sur l'acheminement d'une demande d'un point d'accès multi-régions, consultez the section called “Routage des demandes”.

Si vous voulez que le point d'accès multi-régions puisse récupérer l'objet quel que soit le compartiment qui reçoit la requête, vous devez configurer la réplication entre régions (CRR) d'Amazon S3.

Par exemple, prenons un point d'accès multi-régions avec trois compartiments :

- Un compartiment nommé *amzn-s3-demo-bucket1* dans la région US West (Oregon) qui contient un objet my-image.jpg
- Un compartiment nommé *amzn-s3-demo-bucket2* dans la région Asia Pacific (Mumbai) qui contient un objet my-image.jpg
- Un compartiment nommé *amzn-s3-demo-bucket* dans la région Europe (Frankfurt) qui ne contient pas l'objet my-image.jpg

Dans cette situation, si vous faites une demande GetObjectpour l'objet my-image.jpg, la réussite de cette demande dépend du compartiment qui reçoit votre demande. Étant donné qu'Amazon S3 ne tient pas compte du contenu de la requête, il se peut que votre requête GetObject soit acheminée vers le compartiment *amzn-s3-demo-bucket* le plus proche. Même si votre objet se trouve dans un compartiment du point d'accès multi-régions, vous obtiendrez une erreur HTTP 404 Not Found [HTTP 404 (Introuvable)], car le compartiment individuel qui a reçu votre requête ne possède pas l'objet.

L'activation de la réplication entre régions (CRR) permet d'éviter ce résultat. Avec les règles de réplication appropriées, l'objet my-image.jpg est copié dans le compartiment *amzn-s3-demo-bucket*. Par conséquent, si Amazon S3 achemine votre requête vers ce compartiment, vous pouvez maintenant récupérer l'objet.

La réplication fonctionne normalement avec des compartiments qui sont affectés à un point d'accès multi-Régions. Amazon S3 n'effectue pas de traitement spécial de réplication avec les compartiments qui se trouvent dans des points d'accès multi-régions. Pour en savoir plus sur la configuration de la réplication dans vos compartiments, consultez Présentation de la configuration de la réplication en direct.

Recommandations pour l'utilisation de la réplication avec des points d'accès multi-régions

Pour obtenir les meilleures performances de réplication lorsque vous travaillez avec des points d'accès multi-régions, nous vous recommandons ce qui suit :

- Configurez le contrôle du temps de réplication S3 (S3 RTC). Pour répliquer vos données sur différentes régions dans un délai prévisible, vous pouvez utiliser S3 RTC. Le contrôle du délai de

réplication S3 permet de répliquer 99,99 % des nouveaux objets stockés dans Simple Storage Service (Amazon S3) dans les 15 minutes (conformément à un contrat de niveau de service (SLA)). Pour de plus amples informations, veuillez consulter the section called "Utiliser le contrôle du délai de réplication S3". Des frais supplémentaires sont facturés pour l'utilisation de S3 RTC. Pour plus d'informations, consultez Tarification Amazon S3.

- Utilisez la réplication bidirectionnelle pour maintenir les compartiments synchronisés lorsque les compartiments sont mis à jour par le point d'accès multi-régions. Pour de plus amples informations, veuillez consulter the section called "Création de règles de réplication bidirectionnelle pour votre point d'accès multi-régions".
- Créez des points d'accès multi-régions intercompte pour répliquer des données dans des compartiments dans différents Comptes AWS. Cette approche permet une séparation au niveau des comptes, de sorte que les données peuvent être consultées et répliquées sur différents comptes dans différentes régions autres que le compartiment source. La configuration de points d'accès multi-régions intercompte n'entraîne aucun coût supplémentaire. Si vous êtes propriétaire d'un compartiment mais que vous ne possédez pas le point d'accès multi-régions, vous ne payez que les frais de transfert de données et de demande. Les propriétaires de points d'accès multi-régions paient pour l'acheminement des données et les coûts d'accélération d'Internet. Pour plus d'informations, consultez Tarification Amazon S3.
- Activez la synchronisation des modifications des réplicas pour chaque règle de réplication afin de synchroniser également les modifications des métadonnées de vos objets. Pour plus d'informations, consultez Enabling replica modification sync (Activation de la synchronisation des modifications de réplicas).
- Activez Amazon CloudWatch Metrics pour surveiller les événements de réplication. CloudWatch des frais de mesure s'appliquent. Pour plus d'informations, consultez les CloudWatchtarifs Amazon.

Rubriques

- Création de règles de réplication unidirectionnelle pour votre point d'accès multi-régions
- Création de règles de réplication bidirectionnelle pour votre point d'accès multi-régions
- Affichage des règles de réplication pour votre point d'accès multi-régions

Création de règles de réplication unidirectionnelle pour votre point d'accès multi-régions

Les règles de réplication permettent de copier automatiquement et de manière asynchrone les objets d'un compartiment à l'autre. Une règle de réplication unidirectionnelle permet de garantir que les

données sont entièrement répliquées depuis un compartiment source situé dans un compartiment Région AWS vers un compartiment de destination situé dans une autre région. Lorsque la réplication unidirectionnelle est configurée, une règle de réplication du compartiment source (*amzn-s3-demo-bucket*) vers le compartiment de destination (*amzn-s3-demo-bucket*) est créée. Comme toutes les règles de réplication, vous pouvez appliquer la règle de réplication unidirectionnelle à l'ensemble du compartiment Amazon S3 ou à un sous-ensemble d'objets filtrés par un préfixe ou des étiquettes d'objet.

> **Important**
>
> Nous vous recommandons d'utiliser la réplication unidirectionnelle si vos utilisateurs ne consomment que des objets de vos compartiments de destination. Si vos utilisateurs doivent télécharger ou modifier les objets de vos compartiments de destination, utilisez la réplication bidirectionnelle pour synchroniser tous vos compartiments. Nous recommandons également la réplication bidirectionnelle si vous prévoyez d'insérer le point d'accès multi-régions à des fins de basculement. Pour configurer la réplication bidirectionnelle, consultez the section called “Création de règles de réplication bidirectionnelle pour votre point d'accès multi-régions”.

Pour créer une règle de réplication unidirectionnelle pour votre point d'accès multi-régions

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Choisissez le nom de votre point d'accès multi-régions.
4. Choisissez l'onglet Replication and failover (Réplication et basculement).
5. Faites défiler l'écran jusqu'à la section Replication rules (Règles de réplication), puis sélectionnez Create replication rules (Créer des règles de réplication). Assurez-vous que vous disposez des autorisations suffisantes pour créer la règle de réplication. Dans le cas contraire, la gestion des versions sera désactivée.

   > **Note**
   >
   > Vous pouvez créer des règles de réplication uniquement pour les compartiments dans votre compte. Pour créer des règles de réplication pour des compartiments externes,

les propriétaires des compartiments doivent créer les règles de réplication pour ces compartiments.

6. Sur la page Créer des règles de réplication, choisissez le modèle Répliquer les objets d'un ou de plusieurs compartiments sources vers un ou plusieurs compartiments de destination.

> **Important**
>
> Lorsque vous créez des règles de réplication à l'aide de ce modèle, elles remplacent toutes les règles de réplication existantes qui sont déjà affectées au compartiment. Pour ajouter ou modifier une règle de réplication existante au lieu de la remplacer, accédez à l'onglet Management (Gestion) de chaque compartiment dans la console, puis modifiez la règle dans la section Replication rules (Règles de réplication). Vous pouvez également ajouter ou modifier des règles de réplication existantes à l'aide de l'API AWS CLI SDKs,, ou REST. Pour de plus amples informations, veuillez consulter Éléments du fichier de configuration de réplication.

7. Dans la section Source et destination, sous Compartiments source, sélectionnez un ou plusieurs compartiments à partir desquels vous souhaitez répliquer les objets. Tous les compartiments (source et destination) choisis pour la réplication doivent avoir l'option de gestion des versions S3 activée, et chaque compartiment doit résider dans une Région AWS différente. Pour plus d'informations sur la gestion des versions S3, consultez la section Using versioning in Amazon S3 buckets (Utilisation de la la gestion des versions dans les compartiments Amazon S3).

   Sous Compartiments de destination, sélectionnez un ou plusieurs compartiments à partir desquels vous souhaitez répliquer les objets.

8. Dans la section Replication rule configuration (Configuration de la règle de réplication), choisissez si la règle de réplication sera Enabled (Activée) ou Disabled (Désactivée) lors de sa création.

> **Note**
>
> Vous ne pouvez pas saisir de nom dans la case Replication rule name (Nom de la règle de réplication). Les noms des règles de réplication sont générés en fonction de votre configuration lorsque vous créez la règle de réplication.

9. Dans la section Scope (Étendue), choisissez l'étendue appropriée pour votre réplication.

- Pour répliquer l'ensemble du compartiment, choisissez Apply to all objects in the bucket (Appliquer à tous les objets du compartiment).
- Pour répliquer un sous-ensemble des objets du compartiment, sélectionnez Limit the scope of this rule using one or more filters (Limiter l'étendue de cette règle à l'aide d'un ou plusieurs filtres).

  Vous pouvez filtrer vos objets en utilisant un préfixe, des étiquettes d'objets ou une combinaison des deux.

  - Pour limiter la réplication à tous les objets dont le nom commence par la même chaîne (par exemple `pictures`), saisissez un préfixe dans la case Prefix (Préfixe).

    Si vous saisissez un préfixe correspondant à un nom de dossier, vous devez insérer un caractère `/` à la fin pour indiquer son niveau de hiérarchie (par exemple, `pictures/`). Pour plus d'informations sur les préfixes, consultez Organisation des objets à l'aide de préfixes.
  - Pour répliquer tous les objets avec une ou plusieurs étiquettes d'objet, sélectionnez Add tag (Ajouter une étiquette) et saisissez la paire clé-valeur dans les zones. Pour ajouter une autre étiquette, répétez la procédure. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.

10. Faites défiler vers le bas jusqu'à la section Additional replication options (Options de réplication supplémentaires), puis sélectionnez les options de réplication que vous souhaitez appliquer.

> **Note**
>
> Nous vous recommandons d'appliquer les options suivantes :
>
> - Replication time control (RTC) [Contrôle du temps de réplication (RTC)] : pour répliquer vos données sur différentes régions dans un délai prévisible, vous pouvez utiliser le contrôle du temps de réplication S3 (S3 RTC). Le contrôle du délai de réplication S3 permet de répliquer 99,99 % des nouveaux objets stockés dans Simple Storage Service (Amazon S3) dans les 15 minutes (conformément à un contrat de niveau de service (SLA)). Pour de plus amples informations, veuillez consulter the section called "Utiliser le contrôle du délai de réplication S3".
> - Mesures et notifications de réplication : activez CloudWatch les métriques Amazon pour surveiller les événements de réplication.
> - Réplication des marqueurs de suppression : les marqueurs de suppression créés par les opérations de suppression de S3 seront répliqués. Les marqueurs de suppression

créés par les règles de cycle de vie ne sont pas répliqués. Pour plus d'informations, consultez Répliquer des marqueurs de suppression entre les compartiments.

Des frais supplémentaires s'appliquent au RTC S3 ainsi qu'aux métriques et notifications de CloudWatch réplication. Pour plus d'informations, consultez les sections Tarification Amazon S3 et CloudWatch Tarification Amazon.

11. Si vous écrivez une nouvelle règle de réplication qui remplace une règle existante, sélectionnez I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten (Je reconnais qu'en choisissant l'option Créer des règles de réplication, ces règles de réplication existantes seront écrasées).
12. Choisissez Créer des règles de réplication pour créer et enregistrer votre nouvelle règle de réplication unidirectionnelle.

Création de règles de réplication bidirectionnelle pour votre point d'accès multi-régions

Les règles de réplication permettent de copier automatiquement et de manière asynchrone les objets d'un compartiment à l'autre. Une règle de réplication bidirectionnelle garantit que les données sont entièrement synchronisées entre deux ou plusieurs compartiments dans différentes Régions AWS. Lorsque la réplication bidirectionnelle est configurée, le système crée une règle de réplication du compartiment source (DOC-EXAMPLE-BUCKET-1) vers le compartiment contenant les réplicas (DOC-EXAMPLE-BUCKET-2). Ensuite, une deuxième règle de réplication est créée depuis le compartiment contenant les réplicas (DOC-EXAMPLE-BUCKET-2) vers le compartiment source (DOC-EXAMPLE-BUCKET-1).

Comme toutes les règles de réplication, vous pouvez appliquer la règle de réplication bidirectionnelle à l'ensemble du compartiment Amazon S3 ou à un sous-ensemble d'objets filtrés par un préfixe ou des étiquettes d'objet. Vous pouvez également synchroniser les modifications des métadonnées de vos objets en activant la synchronisation des modifications des réplicas pour chaque règle de réplication. Vous pouvez activer la synchronisation des modifications des répliques via la console Amazon S3 AWS CLI AWS SDKs, l'API REST Amazon S3 ou AWS CloudFormation.

Pour surveiller la progression de la réplication des objets et des métadonnées des objets dans Amazon CloudWatch, activez les métriques et les notifications de réplication S3. Pour plus d'informations, consultez Monitoring progress with replication metrics and Amazon S3 event notifications (Suivi de la progression avec les métriques de réplication et les notifications d'événements Amazon S3).

Pour créer une règle de réplication bidirectionnelle pour votre point d'accès multi-régions

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Choisissez le nom du point d'accès multi-régions que vous souhaitez mettre à jour.
4. Choisissez l'onglet Replication and failover (Réplication et basculement).
5. Faites défiler l'écran jusqu'à la section Replication rules (Règles de réplication), puis sélectionnez Create replication rules (Créer des règles de réplication).
6. Sur la page Create replication rules (Créer des règles de réplication), choisissez le modèle Replicate objects among all specified buckets (Répliquer les objets parmi tous les compartiments spécifiés). Le modèle Replicate objects among all specified buckets (Répliquer les objets parmi tous les compartiments spécifiés) configure une réplication bidirectionnelle (avec des capacités de basculement) pour vos compartiments.

   > **Important**
   >
   > Lorsque vous créez des règles de réplication à l'aide de ce modèle, elles remplacent toutes les règles de réplication existantes qui sont déjà affectées au compartiment. Pour ajouter ou modifier une règle de réplication existante au lieu de la remplacer, accédez à l'onglet Management (Gestion) de chaque compartiment dans la console, puis modifiez la règle dans la section Replication rules (Règles de réplication). Vous pouvez également ajouter ou modifier des règles de réplication existantes à l'aide de l'API REST AWS CLI AWS SDKs,, ou Amazon S3. Pour de plus amples informations, veuillez consulter Éléments du fichier de configuration de réplication.

7. Dans la section Buckets (Compartiments), sélectionnez au moins deux compartiments à partir desquels vous souhaitez répliquer des objets. Tous les compartiments choisis pour la réplication doivent avoir l'option gestion des versions S3 activée, et chaque compartiment doit résider dans une Région AWS différente. Pour plus d'informations sur la gestion des versions S3, consultez la section Using versioning in Amazon S3 buckets (Utilisation de la la gestion des versions dans les compartiments Amazon S3).

> **Note**
>
> Assurez-vous de disposer des autorisations de lecture et de réplication requises pour établir la réplication, sinon vous risquez de rencontrer des erreurs. Pour plus d'informations, consultez Création d'un rôle IAM.

8. Dans la section Replication rule configuration (Configuration de la règle de réplication), choisissez si la règle de réplication sera Enabled (Activée) ou Disabled (Désactivée) lors de sa création.

> **Note**
>
> Vous ne pouvez pas saisir de nom dans la case Replication rule name (Nom de la règle de réplication). Les noms des règles de réplication sont générés en fonction de votre configuration lorsque vous créez la règle de réplication.

9. Dans la section Scope (Étendue), choisissez l'étendue appropriée pour votre réplication.

   - Pour répliquer l'ensemble du compartiment, choisissez Apply to all objects in the bucket (Appliquer à tous les objets du compartiment).
   - Pour répliquer un sous-ensemble des objets du compartiment, sélectionnez Limit the scope of this rule using one or more filters (Limiter l'étendue de cette règle à l'aide d'un ou plusieurs filtres).

     Vous pouvez filtrer vos objets en utilisant un préfixe, des étiquettes d'objets ou une combinaison des deux.

     - Pour limiter la réplication à tous les objets dont le nom commence par la même chaîne (par exemple `pictures`), saisissez un préfixe dans la case Prefix (Préfixe).

       Si vous entrez un préfixe correspondant à un nom de dossier, vous devez insérer le caractère `/` (barre oblique) en tant que dernier caractère (par exemple, `pictures/`).
     - Pour répliquer tous les objets avec une ou plusieurs étiquettes d'objet, sélectionnez Add tag (Ajouter une étiquette) et saisissez la paire clé-valeur dans les zones. Pour ajouter une autre étiquette, répétez la procédure. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.

10. Faites défiler vers le bas jusqu'à la section Additional replication options (Options de réplication supplémentaires), puis sélectionnez les options de réplication que vous souhaitez appliquer.

> **Note**
>
> Nous vous recommandons d'appliquer les options suivantes, en particulier si vous avez l'intention de configurer votre point d'accès multi-régions pour prendre en charge le basculement :
>
> - Replication time control (RTC) [Contrôle du temps de réplication (RTC)] : pour répliquer vos données sur différentes régions dans un délai prévisible, vous pouvez utiliser le contrôle du temps de réplication S3 (S3 RTC). Le contrôle du délai de réplication S3 permet de répliquer 99,99 % des nouveaux objets stockés dans Simple Storage Service (Amazon S3) dans les 15 minutes (conformément à un contrat de niveau de service (SLA)). Pour de plus amples informations, veuillez consulter the section called "Utiliser le contrôle du délai de réplication S3".
> - Mesures et notifications de réplication : activez CloudWatch les métriques Amazon pour surveiller les événements de réplication.
> - Réplication des marqueurs de suppression : les marqueurs de suppression créés par les opérations de suppression de S3 seront répliqués. Les marqueurs de suppression créés par les règles de cycle de vie ne sont pas répliqués. Pour plus d'informations, consultez Répliquer des marqueurs de suppression entre les compartiments.
> - Replica modification sync (Synchronisation des modifications de réplicas) : activez la synchronisation des modifications des réplicas pour chaque règle de réplication afin de synchroniser également les modifications des métadonnées de vos objets. Pour plus d'informations, consultez Enabling replica modification sync (Activation de la synchronisation des modifications de réplicas).
>
> Des frais supplémentaires s'appliquent au RTC S3 ainsi qu'aux métriques et notifications de CloudWatch réplication. Pour plus d'informations, consultez les sections Tarification Amazon S3 et CloudWatchTarification Amazon.

11. Si vous écrivez une nouvelle règle de réplication qui remplace une règle existante, sélectionnez I acknowledge that by choosing Create replication rules, these existing replication rules will be overwritten (Je reconnais qu'en choisissant l'option Créer des règles de réplication, ces règles de réplication existantes seront écrasées).
12. Choisissez Create replication rules (Créer des règles de réplication) pour créer et enregistrer vos nouvelles règles de réplication bidirectionnelle.

Affichage des règles de réplication pour votre point d'accès multi-régions

Avec les points d'accès multi-régions, vous pouvez configurer des règles de réplication unidirectionnelles ou des règles de réplication bidirectionnelles. Pour plus d'informations sur la gestion de vos règles de réplication, consultez Gérer les règles de réplication à l'aide de la console Amazon S3.

Pour afficher des règles de réplication pour votre point d'accès multi-régions

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Multi-Region Access Points (Points d'accès multi-régions).
3. Choisissez le nom de votre point d'accès multi-régions.
4. Choisissez l'onglet Replication and failover (Réplication et basculement).
5. Faites défiler jusqu'à la section Règles de réplication. Cette section répertorie toutes les règles de réplication créées pour votre point d'accès multi-régions.

> **Note**
>
> Si vous avez ajouté un compartiment provenant d'un autre compte à ce point d'accès multi-régions, vous devez disposer de l'autorisation `s3:GetBucketReplication` du propriétaire du compartiment pour consulter les règles de réplication de ce compartiment.

Utilisation de points d'accès multi-régions avec des opérations d'API prises en charge

Amazon S3 fournit un ensemble d'opérations permettant de gérer les points d'accès multi-régions. Amazon S3 traite certaines de ces opérations de manière synchrone et d'autres de manière asynchrone. Lorsque vous invoquez une opération asynchrone, Amazon S3 autorise d'abord l'opération demandée de manière synchrone. Si l'autorisation réussit, Amazon S3 renvoie un jeton que vous pourrez utiliser pour suivre la progression et les résultats de l'opération demandée.

> **Note**
>
> Les demandes effectuées via la console Amazon S3 sont toujours synchrones. La console attend que la demande soit terminée avant de vous autoriser à envoyer une autre demande.

Vous pouvez consulter l'état actuel et les résultats des opérations asynchrones à l'aide de la console, ou `DescribeMultiRegionAccessPointOperation` dans l' AWS CLI API AWS SDKs REST. Amazon S3 fournit un jeton de suivi dans la réponse à une opération asynchrone. Vous devrez inclure ce jeton de suivi en tant qu'argument de `DescribeMultiRegionAccessPointOperation`. Quand vous incluez le jeton de suivi, Amazon S3 renvoie ensuite le statut actuel et les résultats de l'opération spécifiée, notamment les éventuelles erreurs ou informations pertinentes sur les ressources. Amazon S3 effectue les opérations `DescribeMultiRegionAccessPointOperation` de manière synchrone.

Toutes les demandes du plan de contrôle de création ou de gestion de points d'accès multirégions doivent être routées vers la région `US West (Oregon)`. Pour les demandes de plan de données de points d'accès multirégions, il n'est pas nécessaire de spécifier les régions. Pour le plan de contrôle de basculement des points d'accès multirégions, la demande doit être routée vers l'une des cinq régions prises en charge. Pour plus d'informations sur les régions prises en charge par les points d'accès multirégionaux, consultez Restrictions et limitations des points d'accès multi-régions.

En outre, vous devez accorder l'`s3:ListAllMyBuckets`autorisation à l'utilisateur, au rôle ou à toute autre entité AWS Identity and Access Management (IAM) qui fait une demande de gestion d'un point d'accès multirégional.

Les exemples suivants montrent comment utiliser des points d'accès multi-régions avec des opérations compatibles dans Amazon S3.

Rubriques

- Compatibilité des points d'accès multirégionaux avec et Services AWSAWS SDKs
- Compatibilité du point d'accès multi-régions avec les opérations S3
- Visualisez la configuration du routage de votre point d'accès multi-régions.
- Mettez à jour votre politique de compartiment Amazon S3 sous-jacente.
- Mise à jour de la configuration des itinéraires d'un point d'accès multi-régions
- Ajouter un objet à un compartiment dans votre point d'accès multirégion
- Récupération d'objets depuis votre point d'accès multirégion
- Liste des objets stockés dans un compartiment sous-jacent à votre point d'accès multirégion
- Utiliser une URL présignée avec des points d'accès multi-régions
- Utiliser un compartiment configuré avec Requester Pays avec des points d'accès multi-régions

Compatibilité des points d'accès multirégionaux avec et Services AWSAWS SDKs

Pour utiliser un point d'accès multirégional avec des applications qui nécessitent un nom de compartiment Amazon S3, utilisez le nom de ressource Amazon (ARN) du point d'accès multirégional lorsque vous effectuez des demandes à l'aide d'un AWS SDK. Pour vérifier lesquels AWS SDKs sont compatibles avec les points d'accès multirégionaux, voir Compatibilité avec AWS SDKs.

Compatibilité du point d'accès multi-régions avec les opérations S3

Vous pouvez utiliser les opérations d'API du plan de données Amazon S3 suivantes pour effectuer des actions sur des objets dans des compartiments associés à votre point d'accès multirégion. Les opérations S3 suivantes peuvent accepter un point ARNs d'accès multirégional :

- AbortMultipartUpload
- CompleteMultipartUpload
- CreateMultipartUpload
- DeleteObject
- DeleteObjectTagging
- GetObject
- GetObjectAcl
- GetObjectLegalHold
- GetObjectRetention
- GetObjectTagging
- HeadObject
- ListMultipartUploads
- ListObjectsV2
- ListParts
- PutObject
- PutObjectAcl
- PutObjectLegalHold
- PutObjectRetention
- PutObjectTagging
- RestoreObject

- UploadPart

> **Note**
>
> Les points d'accès multirégionaux prennent en charge les opérations de copie utilisant des points d'accès multirégionaux uniquement comme destination lors de l'utilisation de l'ARN du point d'accès multirégional.

Vous pouvez utiliser les opérations de plan de contrôle Amazon S3 suivantes pour créer et gérer vos points d'accès multirégions :

- CreateMultiRegionAccessPoint
- DescribeMultiRegionAccessPointOperation
- GetMultiRegionAccessPoint
- GetMultiRegionAccessPointPolicy
- GetMultiRegionAccessPointPolicyStatus
- GetMultiRegionAccessPointRoutes
- ListMultiRegionAccessPoints
- PutMultiRegionAccessPointPolicy
- SubmitMultiRegionAccessPointRoutes

Visualisez la configuration du routage de votre point d'accès multi-régions.

AWS CLI

L'exemple de commande suivant récupère la configuration de l'itinéraire de votre point d'accès multi-régions afin que vous puissiez voir les statuts de routage actuels de vos compartiments. Pour utiliser cet exemple de commande, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control get-multi-region-access-point-routes
--region eu-west-1
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
```

SDK for Java

Le kit SDK suivant pour le code Java récupère la configuration de l'itinéraire de votre point d'accès multi-régions afin que vous puissiez voir les statuts de routage actuels de vos compartiments. Pour utiliser cet exemple de syntaxe, remplacez *user input placeholders* par vos propres informations.

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.US_EAST_1)
    .credentialsProvider(credentialsProvider)
    .build();

GetMultiRegionAccessPointRoutesRequest request =
 GetMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .build();

GetMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.getMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

Le SDK pour le JavaScript code suivant récupère la configuration de votre itinéraire de point d'accès multirégional afin que vous puissiez voir les statuts de routage actuels de vos buckets. Pour utiliser cet exemple de syntaxe, remplacez *user input placeholders* par vos propres informations.

```
const REGION = 'us-east-1'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new GetMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
      })
    )
```

```
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

Le kit SDK suivant pour le code Python récupère la configuration des itinéraires de votre point d'accès multi-régions afin que vous puissiez voir les statuts de routage actuels de vos compartiments. Pour utiliser cet exemple de syntaxe, remplacez *user input placeholders* par vos propres informations.

```
s3.get_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap)['Routes']
```

Mettez à jour votre politique de compartiment Amazon S3 sous-jacente.

Pour accorder un accès approprié, vous devez également mettre à jour la politique sous-jacente du compartiment Amazon S3. Les exemples suivants délèguent le contrôle d'accès à la politique du point d'accès multi-régions. Une fois que vous avez délégué le contrôle d'accès à la politique de point d'accès multi-régions, la politique de compartiment n'est plus utilisée pour le contrôle d'accès lors de demandes effectuées via ce point d'accès.

Voici un exemple de politique de compartiment qui délègue le contrôle d'accès à la politique de point d'accès multi-régions. Pour utiliser cet exemple de politique de compartiment, remplacez *user input placeholders* par vos propres informations. Pour appliquer cette politique par le biais de la AWS CLI `put-bucket-policy` commande, comme indiqué dans l'exemple suivant, enregistrez la politique dans un fichier, par exemple`policy.json`.

JSON

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

```
    "Principal": { "AWS": "*" },
    "Effect": "Allow",
    "Action": ["s3:*"],
    "Resource": ["arn:aws:s3:::111122223333/*", "arn:aws:s3:::example-s3-
bucket;"],
    "Condition": {
      "StringEquals": {
        "s3:DataAccessPointAccount": "444455556666"
      }
    }
  }
}
```

L'exemple de commande `put-bucket-policy` suivant associe la politique de compartiment S3 mise à jour à votre compartiment S3 :

```
aws s3api put-bucket-policy
  --bucket amzn-s3-demo-bucket
  --policy file:///tmp/policy.json
```

Mise à jour de la configuration des itinéraires d'un point d'accès multi-régions

L'exemple de commande suivant met à jour la configuration des itinéraires du point d'accès multi-régions. Les commandes d'itinéraire des points d'accès multi-régions peuvent être exécutées dans les cinq régions suivantes :

- `ap-southeast-2`
- `ap-northeast-1`
- `us-east-1`
- `us-west-2`
- `eu-west-1`

Dans une configuration de routage de point d'accès multi-régions, vous pouvez définir des compartiments avec un statut de routage actif ou passif. Les compartiments actifs reçoivent du trafic, tandis que les compartiments passifs n'en reçoivent pas. Vous pouvez définir le statut de routage d'un compartiment en définissant la valeur `TrafficDialPercentage` de ce dernier sur `100` pour actif ou `0` pour passif.

AWS CLI

L'exemple de commande suivant met à jour la configuration du routage de votre point d'accès multi-régions. Dans cet exemple, la valeur *amzn-s3-demo-bucket1* est réglée sur le statut actif et *amzn-s3-demo-bucket2* est réglée sur le statut passif. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control submit-multi-region-access-point-routes
--region ap-southeast-2
--account-id 111122223333
--mrap arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap
--route-updates Bucket=amzn-s3-demo-bucket1,TrafficDialPercentage=100
                Bucket=amzn-s3-demo-bucket2,TrafficDialPercentage=0
```

SDK for Java

Le kit SDK suivant pour le code Java met à jour la configuration de l'itinéraire de votre point d'accès multi-régions. Pour utiliser cet exemple de syntaxe, remplacez *user input placeholders* par vos propres informations.

```
S3ControlClient s3ControlClient = S3ControlClient.builder()
    .region(Region.ap-southeast-2)
    .credentialsProvider(credentialsProvider)
    .build();

SubmitMultiRegionAccessPointRoutesRequest request =
 SubmitMultiRegionAccessPointRoutesRequest.builder()
    .accountId("111122223333")
    .mrap("arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap")
    .routeUpdates(
        MultiRegionAccessPointRoute.builder()
            .region("eu-west-1")
            .trafficDialPercentage(100)
            .build(),
        MultiRegionAccessPointRoute.builder()
            .region("ca-central-1")
            .bucket("111122223333")
            .trafficDialPercentage(0)
            .build()
    )
    .build();
```

```
SubmitMultiRegionAccessPointRoutesResponse response =
 s3ControlClient.submitMultiRegionAccessPointRoutes(request);
```

SDK for JavaScript

Le SDK de JavaScript code suivant met à jour la configuration de votre itinéraire de point d'accès multirégional. Pour utiliser cet exemple de syntaxe, remplacez *user input placeholders* par vos propres informations.

```
const REGION = 'ap-southeast-2'

const s3ControlClient = new S3ControlClient({
  region: REGION
})

export const run = async () => {
  try {
    const data = await s3ControlClient.send(
      new SubmitMultiRegionAccessPointRoutesCommand({
        AccountId: '111122223333',
        Mrap: 'arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap',
        RouteUpdates: [
          {
            Region: 'eu-west-1',
            TrafficDialPercentage: 100,
          },
          {
            Region: 'ca-central-1',
            Bucket: 'amzn-s3-demo-bucket1',
            TrafficDialPercentage: 0,
          },
        ],
      })
    )
    console.log('Success', data)
    return data
  } catch (err) {
    console.log('Error', err)
  }
}

run()
```

SDK for Python

Le kit SDK suivant pour le code Python met à jour la configuration de l'itinéraire de votre point d'accès multi-régions. Pour utiliser cet exemple de syntaxe, remplacez *user input placeholders* par vos propres informations.

```
s3.submit_multi_region_access_point_routes(
        AccountId=111122223333,
        Mrap=arn:aws:s3::111122223333:accesspoint/abcdef0123456.mrap,
        RouteUpdates= [{
            'Bucket': amzn-s3-demo-bucket,
            'Region': ap-southeast-2,
            'TrafficDialPercentage': 10
        }])
```

Ajouter un objet à un compartiment dans votre point d'accès multirégion

Pour ajouter un objet au compartiment associé au point d'accès multirégion, vous pouvez utiliser l'opération PutObject. Pour maintenir synchronisés tous les compartiments dans le point d'accès multirégion, activez la réplication entre régions.

> **Note**
>
> Pour utiliser cette opération, vous devez disposer de l'autorisation `s3:PutObject` pour le point d'accès multirégion. Pour plus d'informations sur les exigences relatives aux autorisations des points d'accès multirégions, consultez Autorisations.

AWS CLI

L'exemple de demande de plan de données suivant charge *example.txt* dans le point d'accès multirégion spécifié. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3api put-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --key example.txt --
body example.txt
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
        .build();

PutObjectRequest objectRequest = PutObjectRequest.builder()
        .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
        .key("example.txt")
        .build();

s3Client.putObject(objectRequest, RequestBody.fromString("Hello S3!"));
```

SDK for JavaScript

```
const client = new S3Client({});

async function putObjectExample() {
    const command = new PutObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt",
        Body: "Hello S3!",
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.put_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt',
    Body='Hello S3!'
)
```

Récupération d'objets depuis votre point d'accès multirégion

Pour récupérer des objets depuis le point d'accès multirégion, vous pouvez utiliser l'opération GetObject.

> **Note**
>
> Pour utiliser cette opération d'API, vous devez disposer de l'autorisation `s3:GetObject` pour le point d'accès multirégion. Pour plus d'informations sur les exigences relatives aux autorisations des points d'accès multirégions, consultez Autorisations.

AWS CLI

L'exemple de demande de plan de données suivant récupère *`example.txt`* depuis le point d'accès multirégion spécifié et le télécharge en tant que *`downloaded_example.txt`*. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3api get-object --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap --
key example.txt downloaded_example.txt
```

SDK for Java

```
S3Client s3 = S3Client
   .builder()
   .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example.txt")
    .build();

s3Client.getObject(getObjectRequest);
```

SDK for JavaScript

```
const client = new S3Client({})

async function getObjectExample() {
```

```
    const command = new GetObjectCommand({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
        Key: "example.txt"
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.get_object(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap',
    Key='example.txt'
)
```

Liste des objets stockés dans un compartiment sous-jacent à votre point d'accès multirégion

Pour renvoyer la liste des objets stockés dans un compartiment sous-jacent à votre point d'accès multirégion, utilisez l'opération ListObjectsV2. Dans l'exemple de commande suivant, tous les objets du point d'accès multirégion spécifié sont répertoriés à l'aide de l'ARN du point d'accès multirégion. Dans ce cas, l'ARN du point d'accès multirégion est :

`arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap`

> **Note**
>
> Pour utiliser cette opération d'API, vous devez disposer de l'autorisation `s3:ListBucket` pour le point d'accès multirégion et le compartiment sous-jacent. Pour plus d'informations sur les exigences relatives aux autorisations des points d'accès multirégions, consultez Autorisations.

AWS CLI

L'exemple de demande de plan de données suivant répertorie les objets présents dans le compartiment sous-jacent au point d'accès multirégion spécifié par l'ARN. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3api list-objects-v2 --bucket
 arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap
```

SDK for Java

```
S3Client s3Client = S3Client.builder()
        .build();

String bucketName = "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap";

ListObjectsV2Request listObjectsRequest = ListObjectsV2Request
    .builder()
    .bucket(bucketName)
    .build();

 s3Client.listObjectsV2(listObjectsRequest);
```

SDK for JavaScript

```
const client = new S3Client({});

async function listObjectsExample() {
    const command = new ListObjectsV2Command({
        Bucket: "arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap",
    });

    try {
        const response = await client.send(command);
        console.log(response);
    } catch (err) {
        console.error(err);
    }
}
```

SDK for Python

```
import boto3

client = boto3.client('s3')
client.list_objects_v2(
    Bucket='arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap'
)
```

Utiliser une URL présignée avec des points d'accès multi-régions

Vous pouvez utiliser une URL présignée pour générer une URL permettant aux autres d'accéder à vos compartiments Amazon S3 via un point d'accès multirégion Amazon S3. Lorsque vous créez une URL présignée, vous l'associez à une action d'objet spécifique, telle qu'un chargement S3 (`PutObject`) ou un téléchargement S3 (`GetObject`). Vous pouvez partager l'URL présignée, et toute personne y ayant accès peut effectuer l'action intégrée dans l'URL comme s'il s'agissait de l'utilisateur connecté d'origine.

Les documents présignés URLs ont une date d'expiration. Lorsque le délai d'expiration est atteint, l'URL ne fonctionne plus.

Avant d'utiliser des points d'accès multirégionaux S3 présignés URLs, vérifiez la compatibilité du AWS SDK avec l'algorithme SigV4A. Vérifiez que la version de votre kit SDK prend en charge SigV4A comme mise en œuvre de la signature qui est utilisée pour signer les requêtes globales Région AWS . Pour plus d'informations sur l'utilisation de Presigned URLs avec Amazon S3, consultez Partage d'objets à l'aide de URLs Presigned.

Les exemples suivants montrent comment utiliser des points d'accès multirégionaux URLs présignés. Pour utiliser ces exemples, remplacez *`user input placeholders`* par vos propres informations.

AWS CLI

```
aws s3 presign
 arn:aws:s3::123456789012:accesspoint/MultiRegionAccessPoint_alias/example-file.txt
```

SDK for Python

```
import logging
import boto3
```

```
from botocore.exceptions import ClientError

s3_client = boto3.client('s3',aws_access_key_id='xxx',aws_secret_access_key='xxx')
s3_client.generate_presigned_url(HttpMethod='PUT',ClientMethod="put_object",
 Params={'Bucket':'arn:aws:s3::123456789012:accesspoint/
abcdef0123456.mrap','Key':'example-file'})
```

SDK for Java

```
S3Presigner s3Presigner = S3Presigner.builder()
    .credentialsProvider(StsAssumeRoleCredentialsProvider.builder()
        .refreshRequest(assumeRole)
        .stsClient(stsClient)
        .build())
    .build();

GetObjectRequest getObjectRequest = GetObjectRequest.builder()
    .bucket("arn:aws:s3::123456789012:accesspoint/abcdef0123456.mrap")
    .key("example-file")
    .build();

GetObjectPresignRequest preSignedReq = GetObjectPresignRequest.builder()
    .getObjectRequest(getObjectRequest)
    .signatureDuration(Duration.ofMinutes(10))
    .build();

PresignedGetObjectRequest presignedGetObjectRequest =
 s3Presigner.presignGetObject(preSignedReq);
```

Note

Pour utiliser SigV4A avec des informations d'identification de sécurité temporaires, par exemple, lorsque vous utilisez des rôles IAM, assurez-vous de demander les informations d'identification temporaires à un point de terminaison régional situé dans AWS Security Token Service (), plutôt qu'à un point de terminaison global.AWS STS Si vous utilisez le point de terminaison global pour AWS STS (`sts.amazonaws.com`), AWS STS cela générera des informations d'identification temporaires à partir d'un point de terminaison global, ce qui n'est pas pris en charge par Sig4A. Par conséquent, vous obtenez une erreur. Pour résoudre ce problème, utilisez l'un des points de terminaison régionaux répertoriés pour AWS STS.

Utiliser un compartiment configuré avec Requester Pays avec des points d'accès multi-régions

Si un compartiment S3 associé à vos points d'accès multirégions est configuré pour utiliser le paiement par le demandeur, le demandeur paiera à la fois la demande de compartiment, le téléchargement et tous les coûts liés aux points d'accès multirégions. Pour plus d'informations, consultez Tarification Amazon S3.

Voici un exemple de demande de plan de données adressée à un point d'accès multirégion connecté à un compartiment de type Paiement par le demandeur.

AWS CLI

Pour télécharger des objets à partir d'un point d'accès multirégion connecté à un compartiment de type Paiement par le demandeur, vous devez spécifier `--request-payer requester` dans le cadre de votre demande get-object. Vous devez également spécifier le nom du fichier dans le compartiment, ainsi que l'emplacement où le fichier téléchargé doit être stocké.

```
aws s3api get-object --bucket MultiRegionAccessPoint_ARN --request-payer requester
 --key example-file-in-bucket.txt example-location-of-downloaded-file.txt
```

SDK for Java

Pour télécharger des objets à partir d'un point d'accès multirégion connecté à un compartiment de type Paiement par le demandeur, vous devez spécifier `RequestPayer.REQUESTER` dans le cadre de votre demande `GetObject`. Vous devez également spécifier le nom du fichier dans le compartiment, ainsi que l'emplacement où il doit être stocké.

```
GetObjectResponse getObjectResponse = s3Client.getObject(GetObjectRequest.builder()
    .key("example-file.txt")
    .bucket("arn:aws:s3::
123456789012:accesspoint/abcdef0123456.mrap")
    .requestPayer(RequestPayer.REQUESTER)
    .build()
).response();
```

Surveillance et journalisation des demandes effectuées via un point d'accès multi-Régions vers les ressources sous-jacentes

Amazon S3 journalise les demandes effectuées via les points d'accès multi-régions et les demandes adressées aux opérations d'API qui les gèrent, telles que `CreateMultiRegionAccessPoint`

et `GetMultiRegionAccessPointPolicy`. Les demandes adressées à Amazon S3 via un point d'accès multirégional apparaissent dans les journaux d'accès de votre serveur Amazon S3 et AWS CloudTrail portent le nom d'hôte du point d'accès multirégional. Le nom d'hôte d'un point d'accès prend la forme *`MRAP_alias`*`.accesspoint.s3-global.amazonaws.com`. Par exemple, supposons que vous disposez de la configuration de compartiment et de point d'accès multi-Régions suivante :

- Un compartiment nommé `my-bucket-usw2` dans la région `us-west-2` qui contient un objet `my-image.jpg`.
- Un compartiment nommé `my-bucket-aps1` dans la région `ap-south-1` qui contient un objet `my-image.jpg`.
- Un compartiment nommé `my-bucket-euc1` dans la région `eu-central-1` qui ne contient pas d'objet nommé `my-image.jpg`.
- Un point d'accès multi-Régions nommé `my-mrap`avec l'alias `mfzwi23gnjvgw.mrap` qui est configuré pour traiter les demandes des trois compartiments.
- L'identifiant AWS de votre compte est`123456789012`.

Une demande effectuée pour récupérer `my-image.jpg` directement via le compartiment apparaît dans vos journaux avec un nom d'hôte *`bucket_name`*`.s3.`*`Region`*`.amazonaws.com`.

Si vous faites la demande par le biais du point d'accès multi-régions, Amazon S3 détermine d'abord lequel des compartiments des différentes régions est le plus proche. Une fois qu'Amazon S3 aura déterminé le compartiment à utiliser pour traiter la demande, il enverra la demande à ce compartiment et journalisera l'opération à l'aide du nom d'hôte du point d'accès multi-régions. Dans cet exemple, si Amazon S3 relaye la demande à `my-bucket-aps1`, vos journaux refléteront une demande `GET` réussie pour `my-image.jpg` depuis `my-bucket-aps1`, en utilisant un nom d'hôte de `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`.

> **Important**
>
> Les points d'accès multi-régions ne connaissent pas le contenu des données des compartiment sous-jacents. Par conséquent, le compartiment qui reçoit la demande peut ne pas contenir les données demandées. Par exemple, si Amazon S3 détermine que le compartiment `my-bucket-euc1` est le plus proche, vos journaux indiqueront l'échec d'une demande `GET` pour `my-image.jpg`, depuis `my-bucket-euc1`, avec un nom d'hôte de `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`. Si la demande

a été acheminée vers `my-bucket-usw2` au lieu de cela, vos journaux indiqueraient une demande `GET` réussie.

Pour en savoir plus sur les journaux d'accès au serveur Amazon S3, consultez Enregistrement de demandes avec journalisation des accès au serveur. Pour plus d'informations AWS CloudTrail, voir Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

Surveillance et journalisation des demandes faites aux opérations d'API de gestion de points d'accès multi-régions

Amazon S3 fournit plusieurs opérations d'API de gestion des points d'accès multi-régions, telles que `CreateMultiRegionAccessPoint` et `GetMultiRegionAccessPointPolicy`. Lorsque vous envoyez des demandes à ces opérations d'API à l'aide de AWS Command Line Interface (AWS CLI) AWS SDKs, ou de l'API REST Amazon S3, Amazon S3 traite ces demandes de manière asynchrone. Si vous disposez des autorisations appropriées pour la demande, Amazon S3 renverra un jeton pour ces demandes. Vous pouvez utiliser ce jeton avec `DescribeAsyncOperation` pour vous aider à afficher le statut des opérations asynchrones en cours. Amazon S3 traite `DescribeAsyncOperation` de manière synchrone. Pour consulter l'état des demandes asynchrones, vous pouvez utiliser la console Amazon S3 ou l' AWS CLI API SDKs REST.

> **Note**
>
> La console affiche uniquement l'état des demandes asynchrones effectuées au cours des 14 jours précédents. Pour consulter le statut des anciennes demandes, utilisez l'API AWS CLI SDKs, ou REST.

Les opérations de gestion asynchrone peuvent avoir l'un des états suivants :

NEW

Amazon S3 a reçu la demande et se prépare à effectuer l'opération.

IN_PROGRESS

Amazon S3 effectue actuellement l'opération.

SUCCESS

L'opération a réussi. La réponse inclut des informations pertinentes, telles que l'alias de point d'accès multi-Régions pour une demande `CreateMultiRegionAccessPoint`.

FAILED

L'opération a échoué. La réponse inclut un message d'erreur indiquant la raison de l'échec de la demande.

Utilisation AWS CloudTrail avec des points d'accès multirégionaux

Vous pouvez l'utiliser AWS CloudTrail pour afficher, rechercher, télécharger, archiver, analyser et répondre à l'activité des comptes dans l'ensemble de votre AWS infrastructure. Grâce aux points d'accès multirégionaux et à la CloudTrail journalisation, vous pouvez identifier les éléments suivants :

- Qui ou quoi a pris quelle mesure
- Quelles ressources ont été utilisées
- Moment où l'événement est survenu
- Autres détails concernant l'événement

Vous pouvez utiliser ces informations de journalisation pour vous aider à analyser les activités qui se sont produites via vos points d'accès multi-régions et à y répondre.

Comment configurer les points AWS CloudTrail d'accès multirégionaux

Pour activer la CloudTrail journalisation pour toutes les opérations liées à la création ou à la maintenance de points d'accès multirégionaux, vous devez configurer la CloudTrail journalisation pour enregistrer les événements dans la région de l'ouest des États-Unis (Oregon). Vous devez configurer votre journalisation de cette façon, quelle que soit la région dans laquelle vous vous trouvez lorsque vous effectuez la demande, ou quelles que soient les régions prises en charge par le point d'accès multi-régions. Toutes les demandes de création ou de gestion d'un point d'accès multi-régions sont acheminées via la région USA Ouest (Oregon). Nous vous recommandons d'ajouter cette région à un journal d'activité existant ou de créer un journal d'activité contenant cette région et toutes les régions associées au point d'accès multi-régions.

Amazon S3 enregistre les demandes de journalisation effectuées via un point d'accès multi-régions et les demandes adressées aux opérations d'API qui gèrent les points d'accès, telles que `CreateMultiRegionAccessPoint` et `GetMultiRegionAccessPointPolicy`. Lorsque vous

enregistrez ces demandes via un point d'accès multirégional, elles apparaissent dans vos AWS CloudTrail journaux avec le nom d'hôte du point d'accès multirégional. Par exemple, si vous envoyez des demandes à un bucket via un point d'accès multirégional avec l'alias`mfzwi23gnjvgw.mrap`, les entrées du CloudTrail journal porteront le nom d'hôte. `mfzwi23gnjvgw.mrap.accesspoint.s3-global.amazonaws.com`

Les points d'accès multirégionaux acheminent les demandes vers le compartiment le plus proche. En raison de ce comportement, lorsque vous consultez les CloudTrail journaux d'un point d'accès multirégional, vous verrez des demandes adressées aux compartiments sous-jacents. Certaines de ces demandes peuvent être des demandes directes vers le compartiment et non acheminées via le point d'accès multi-régions. Gardez ce fait en tête lorsque vous examinez le trafic. Si un compartiment est dans un point d'accès multi-Régions, les demandes pourront toujours être adressées directement à ce compartiment sans passer par le point d'accès multi-Régions.

Des événements asynchrones sont impliqués dans la création et la gestion des points d'accès multi-Régions. Les requêtes asynchrones ne contiennent aucun événement d'achèvement dans le CloudTrail journal. Pour en savoir plus amples sur les demandes asynchrones, consultez Surveillance et journalisation des demandes faites aux opérations d'API de gestion de points d'accès multi-régions.

Pour plus d'informations AWS CloudTrail, voir Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

Conservation de plusieurs versions d’objets grâce à la gestion des versions S3

La gestion des versions Simple Storage Service (Amazon S3) permet de conserver plusieurs variantes d’un objet dans le même compartiment. Vous pouvez utiliser la fonctionnalité de gestion des versions S3 pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans vos compartiments. La gestion des versions permet de récupérer facilement les données en cas d’action involontaire d’un utilisateur ou de défaillance applicative. Lorsque la gestion des versions est activée pour un compartiment, si Simple Storage Service (Amazon S3) reçoit simultanément plusieurs demandes d’écriture pour le même objet, il stocke tous ces objets.

Les compartiments activés pour la gestion des versions vous permettent de récupérer des objets en cas de suppression ou remplacement accidentel. Par exemple, si vous supprimez un objet, Amazon S3 insère un marqueur de suppression au lieu de supprimer l’objet définitivement. Le marqueur de suppression devient la version actuelle de l’objet. Si vous remplacez un objet, cela

crée une nouvelle version d'objet dans le compartiment. Vous pouvez toujours restaurer la version précédente. Pour plus d'informations, consultez Suppression des versions d'objet d'un compartiment activé pour la gestion des versions.

Par défaut, la gestion des versions S3 est désactivé sur les compartiments et vous devez l'activer explicitement. Pour plus d'informations, consultez Activation de la gestion des versions sur les compartiments.

> **Note**
>
> - L'API SOAP ne prend pas en charge la gestion des versions S3. La prise en charge de SOAP via HTTP est obsolète, mais continue d'être disponible sur HTTP. Les nouvelles fonctions Amazon S3 ne sont pas prises en charge pour SOAP.
> - Les tarifs Amazon S3 normaux s'appliquent pour chaque version d'un objet stocké ou transféré. Chaque version d'un objet est l'objet entier ; il ne s'agit pas simplement d'une différence par rapport à la version précédente. Par conséquent, si vous possédez trois versions d'un objet stocké, vous êtes facturé pour trois objets.

Compartiments non versionnés, activés pour la gestion des versions et suspendus

Les compartiments peuvent être dans l'un des trois états suivants :

- Non versionné (valeur par défaut)
- Gestion des versions activée
- Gestion des versions suspendue

L'activation et la suspension de la gestion des versions se fait au niveau du compartiment. Lorsque vous activez un compartiment pour la gestion des versions, il ne peut jamais revenir à un état non versionné. Toutefois, il est possible d'annuler la gestion des versions sur ce compartiment.

L'état de gestion des versions s'applique à tous les objets (jamais à certains) du compartiment. Lorsque vous activez la gestion des versions dans un compartiment, tous les nouveaux objets sont versionnés et reçoivent un ID de version unique. Les objets qui existaient déjà dans le compartiment au moment où la gestion de versions a été activée seront toujours versionnés et dotés d'un ID de version unique lorsqu'ils seront modifiés par des demandes futures. Remarques :

- Les objets qui sont stockés dans le compartiment avant que vous définissiez l'état de la gestion des versions ont un ID de version `null`. Lorsque vous activez la gestion des versions, les objets existants dans le compartiment ne changent pas. Seule la façon dont Amazon S3 gère les objets dans les futures demandes change. Pour plus d'informations, consultez Utiliser des objets dans un compartiment activé pour la gestion des versions.
- Le propriétaire du compartiment (ou tout utilisateur doté des autorisations adaptées) peut désactiver la gestion des versions pour stopper l'accumulation des versions d'objet. Lorsque vous désactivez la gestion des versions, les objets existants du compartiment ne changent pas. Seule la façon dont Amazon S3 gère les objets dans les futures demandes change. Pour plus d'informations, consultez Utilisation des objets dans un compartiment désactivé pour la gestion des versions.

Utilisation de la gestion des versions S3 avec le cycle de vie S3

Pour personnaliser votre approche de la conservation des données et maîtriser les coûts de stockage, utilisez la gestion des versions des objets avec le cycle de vie S3. Pour de plus amples informations, veuillez consulter Gestion du cycle de vie des objets. Pour plus d'informations sur la création de configurations S3 Lifecycle à l'aide de l'API AWS Management Console AWS CLI AWS SDKs,, ou REST, consultezDéfinition d'une configuration du cycle de vie S3 sur un compartiment.

> **Important**
>
> Si vous avez une configuration de cycle de vie d'expiration des objets dans votre compartiment non versionné et que vous souhaitez conserver le même comportement de suppression définitive lorsque vous activez la gestion des versions, vous devez ajouter une configuration d'expiration des versions anciennes. La configuration du cycle de vie d'expiration des versions non actuelles gère les suppressions des versions non actuelles des objets dans le compartiment avec gestion des versions. (Un compartiment avec gestion des versions conserve une version actuelle et aucune, une ou plusieurs versions non actuelles d'un objet.) Pour de plus amples informations, veuillez consulter Définition d'une configuration du cycle de vie S3 sur un compartiment.

Pour en savoir plus sur l'utilisation de la gestion des versions S3, consultez les rubriques suivantes.

Rubriques

- Fonctionnement de la gestion des versions S3

- Activation de la gestion des versions sur les compartiments
- Configuration de la fonction Supprimer MFA
- Utiliser des objets dans un compartiment activé pour la gestion des versions
- Utilisation des objets dans un compartiment désactivé pour la gestion des versions
- Résolution des problèmes de gestion des versions

Fonctionnement de la gestion des versions S3

Vous pouvez utiliser la gestion des versions S3 pour conserver plusieurs versions d'un objet dans un même compartiment afin de pouvoir restaurer des objets qui sont accidentellement supprimés ou remplacés. Par exemple, si vous appliquez la gestion des versions S3 à un compartiment, les modifications suivantes se produisent :

- Si vous supprimez un objet, au lieu de supprimer l'objet définitivement, Amazon S3 insère un marqueur de suppression, qui devient la version d'objet actuelle. Vous pouvez ensuite restaurer la version précédente. Pour plus d'informations, consultez Suppression des versions d'objet d'un compartiment activé pour la gestion des versions.
- Si vous remplacez un objet, Amazon S3 ajoute une nouvelle version d'objet dans le compartiment. La version précédente reste dans le compartiment et devient une version ancienne. Vous pouvez restaurer la version précédente.

> **Note**
>
> Les tarifs Amazon S3 normaux s'appliquent pour chaque version d'un objet stocké et transféré. Chaque version d'un objet est l'objet entier ; il n'est pas différent de la version précédente. Par conséquent, si vous possédez trois versions d'un objet stocké, vous êtes facturé pour trois objets.

Chaque compartiment S3 créé possède une sous-ressource de gestion des versions qui lui est associée. (Pour plus d'informations, consultez Options de configuration des buckets à usage général.) Par défaut, votre compartiment est non versionné, et la sous-ressource de la gestion des versions stocke une configuration de gestion des versions vide, comme suit :

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
```

```
</VersioningConfiguration>
```

Pour activer la gestion des versions, vous pouvez envoyer une demande à Amazon S3 avec une configuration de la gestion des versions qui inclut un statut `Enabled`.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

Pour désactiver la gestion des versions, vous configurez la valeur de l'état sur `Suspended`.

> **Note**
>
> Quand vous activez la gestion des versions sur un compartiment pour la première fois, la propagation complète de la modification peut prendre un court laps de temps. Pendant que cette modification se propage, il est possible que vous rencontriez des erreurs `HTTP 404 NoSuchKey` intermittentes pour les demandes adressées aux objets créés ou mis à jour après l'activation de la gestion des versions. Nous vous recommandons d'attendre 15 minutes après l'activation de la gestion des versions avant d'exécuter des opérations d'écriture (`PUT` ou `DELETE`) sur les objets du compartiment.

Le propriétaire du bucket et tous les utilisateurs autorisés AWS Identity and Access Management (IAM) peuvent activer le versionnement. Le propriétaire du bucket est celui Compte AWS qui a créé le bucket. Pour plus d'informations sur les autorisations, consultez Gestion des identités et des accès pour Amazon S3.

Pour plus d'informations sur l'activation et la désactivation de la gestion des versions S3 à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou REST, consultez. the section called "Activation de la gestion des versions sur les compartiments"

Rubriques

- Version IDs
- Flux de travail de la gestion des versions

Version IDs

Si vous activez la gestion des versions pour un compartiment, Simple Storage Service (Amazon S3) génère automatiquement un ID de version unique pour l'objet qui est stocké. Par exemple, dans un compartiment, vous pouvez avoir deux objets dotés de la même clé (nom de l'objet) mais d'une version différente IDs, par exemple `photo.gif` (version 111111) et `photo.gif` (version 121212). Schéma illustrant un compartiment activé pour la gestion des versions contenant deux objets dotés de la même clé mais d'une version différente. IDs

Chaque objet possède un ID de version, que la gestion des versions S3 soit activée ou non. Si la gestion des versions S3 n'est pas activée, Amazon S3 définit la valeur de l'ID de version sur `null`. Si vous activez la gestion des versions S3, Simple Storage Service (Amazon S3) attribue une valeur d'ID de version à l'objet. Cette valeur distingue l'objet des autres versions de la même clé.

Lorsque vous activez la gestion des versions S3 dans un compartiment existant, les objets déjà stockés dans le compartiment ne changent pas. Leur version IDs (`null`), leur contenu et leurs autorisations restent les mêmes. Après avoir activé la gestion des versions S3, chaque objet ajouté au compartiment obtient un ID de version, qui le distingue des autres versions de la même clé.

Seul Amazon S3 génère des versions IDs et elles ne peuvent pas être modifiées. IDs Les versions sont des chaînes opaques Unicode, codées en UTF-8, prêtes pour les URL, d'une longueur maximale de 1 024 octets. Voici un exemple :

```
3sL4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY+MTRCxf3vjVBH40Nr8X8gdRQBpUMLUo
```

> **Note**
>
> Pour des raisons de simplicité, les autres exemples de cette rubrique sont beaucoup plus courts IDs.

Flux de travail de la gestion des versions

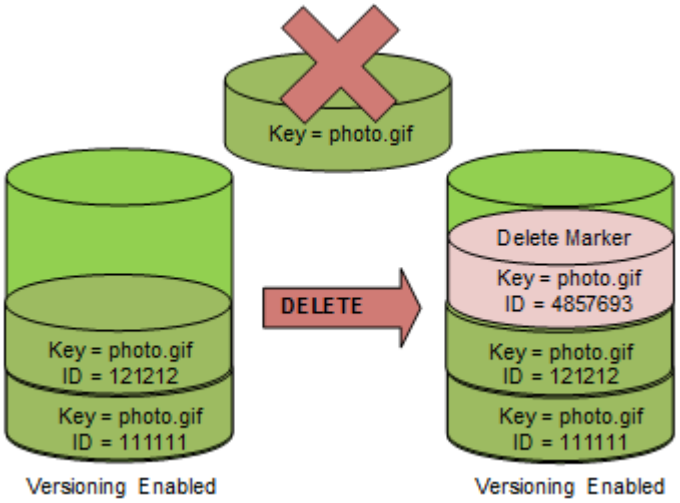
Lorsque vous faites une demande PUT sur un objet dans un compartiment activé pour la gestion des versions, l'ancienne version n'est pas remplacée. Comme le montre la figure suivante, lorsqu'une nouvelle version de `photo.gif` est PUT dans un compartiment qui contient déjà un objet portant le même nom, le comportement suivant se produit :

- L'objet d'origine (ID = 111111) reste dans le compartiment.

- Amazon S3 génère un nouvel ID de version (121212) et ajoute cette nouvelle version de l'objet au compartiment.

Cette fonctionnalité vous permet de récupérer une version précédente d'un objet si celui-ci a été accidentellement remplacé ou supprimé.

Lorsque vous faites une requête `DELETE` sur un objet, toutes les versions restent dans le compartiment et Amazon S3 insère un marqueur de suppression, comme illustré dans le schéma suivant.



Le marqueur de suppression devient la version actuelle de l'objet. Par défaut, les demandes `GET` récupèrent la version la plus récemment stockée. Le fait d'effectuer une requête `GET Object` lorsque la version actuelle est un marqueur de suppression renvoie une erreur `404 Not Found`, comme illustré dans la figure suivante.

Vous pouvez, toutefois, vous pouvez faire une demande `GET` sur une ancienne version d'un objet en spécifiant son ID de version. Dans le schéma suivant, vous faites une demande `GET` sur une version d'objet spécifique, 111111. Amazon S3 renvoie une version d'objet même s'il ne s'agit pas de la version actuelle.

Pour plus d'informations, consultez Récupération de versions d'objets à partir d'un compartiment activé pour la gestion des versions.

Vous pouvez supprimer définitivement un objet en spécifiant la version que vous souhaitez supprimer. Seul le propriétaire d'un compartiment Amazon S3 ou d'un utilisateur IAM autorisé peut supprimer une version de manière définitive. Si votre opération `DELETE` inclut l'élément `versionId`,

cette version de l'objet est définitivement supprimée et Amazon S3 n'insère pas de marqueur de suppression.

Vous pouvez ajouter une sécurité supplémentaire en configurant un compartiment pour activer la suppression par authentification multifactorielle (MFA). Quand vous activez la suppression MFA pour un compartiment, le propriétaire du compartiment doit inclure deux formes d'authentification pour toute demande de suppression d'une version ou de changement de l'état de la gestion des versions du compartiment. Pour plus d'informations, consultez Configuration de la fonction Supprimer MFA.

Quand les nouvelles versions sont-elles créées pour un objet ?

Les nouvelles versions sont créées uniquement lorsque vous faites une requête PUT sur un nouvel objet. Sachez que certaines actions, comme `CopyObject`, fonctionnent en mettant en œuvre une opération PUT.

Certaines actions qui modifient l'objet actuel ne créent pas de nouvelle version, car elles ne font pas de requête PUT sur le nouvel objet. Cela inclut des actions telles que la modification des balises sur un objet.

> **Important**
>
> Si vous remarquez une augmentation importante du nombre de réponses HTTP 503 (Service indisponible) reçues pour les requêtes d'objet PUT ou DELETE Amazon S3 concernant un compartiment pour lequel la gestion des versions S3 est activée, il est possible qu'il y ait un ou plusieurs objets du compartiment avec des millions de versions. Pour plus d'informations, consultez la section sur la gestion des versions S3 de Résolution des problèmes de gestion des versions.

Activation de la gestion des versions sur les compartiments

Vous pouvez utiliser la gestion des versions Simple Storage Service (Amazon S3) pour conserver plusieurs versions d'un objet dans un même compartiment. Cette section fournit des exemples expliquant comment activer le versionnement sur un bucket à l'aide de la console, de l'API REST et AWS Command Line Interface (AWS CLI). AWS SDKs

> **Note**
>
> Après avoir activé la gestion des versions sur un bucket pour la première fois, la propagation complète de la modification dans le système S3 peut prendre jusqu'à 15 minutes. Pendant

ce temps, les GET demandes d'objets créés ou mis à jour après l'activation du versionnement peuvent entraîner des HTTP 404 NoSuchKey erreurs. Nous vous recommandons d'attendre 15 minutes après avoir activé le versionnement avant d'effectuer des opérations d'écriture (PUTouDELETE) sur des objets du compartiment. Cette période d'attente permet d'éviter les problèmes potentiels liés à la visibilité des objets et au suivi des versions.

Pour plus d'informations sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3. Pour en savoir plus sur l'utilisation d'objets se trouvant dans un compartiment dont la gestion des versions est activée, consultez Utiliser des objets dans un compartiment activé pour la gestion des versions.

Pour en savoir plus sur l'utilisation de la gestion des versions S3 pour protéger les données, consultez Tutoriel : protection des données sur Amazon S3 contre les suppressions accidentelles ou les bogues d'application à l'aide de l'archivage par versions S3, du verrouillage d'objets S3 et de la réplication S3.

Chaque compartiment S3 créé possède une sous-ressource de gestion des versions qui lui est associée. (Pour plus d'informations, consultez Options de configuration des buckets à usage général.) Par défaut, votre compartiment est non versionné, et la sous-ressource de la gestion des versions stocke une configuration de gestion des versions vide, comme suit :

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</VersioningConfiguration>
```

Pour activer la gestion des versions, vous pouvez envoyer une demande à Simple Storage Service (Amazon S3) avec une configuration de la gestion des versions qui inclut un statut.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>Enabled</Status>
</VersioningConfiguration>
```

Pour désactiver la gestion des versions, vous configurez la valeur de l'état sur Suspended.

Le propriétaire du compartiment et tous les utilisateurs autorisés peuvent activer la gestion des versions. Le propriétaire du bucket est celui Compte AWS qui a créé le bucket (le compte root). Pour plus d'informations sur les autorisations, consultez Gestion des identités et des accès pour Amazon S3.

Les sections suivantes fournissent plus de détails sur l'activation de la gestion des versions S3 à l'aide de la console AWS CLI, et du AWS SDKs.

Utilisation de la console S3

Procédez comme suit pour utiliser le AWS Management Console afin d'activer le versionnement sur un compartiment S3.

Pour activer ou désactiver la gestion des versions sur un compartiment S3 à usage général

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer le versionnement.
4. Choisissez Propriétés.
5. Sous Bucket Versioning (Gestion des versions de compartiment), choisissez Edit (Modifier).
6. Choisissez Interrompre ou Activer, puis Enregistrer les modifications.

> **Note**
>
> Vous pouvez utiliser l'authentification AWS multifactorielle (MFA) avec le versionnement. Lorsque vous utilisez l'authentification MFA avec le contrôle de version, vous devez fournir vos clés Compte AWS d'accès et un code valide provenant du dispositif MFA du compte pour supprimer définitivement une version d'objet ou suspendre ou réactiver le contrôle de version. Pour utiliser l'authentification multifactorielle (MFA) avec la gestion des versions, vous activez `MFA Delete`. Vous ne pouvez pas activer `MFA Delete` à l'aide de la AWS Management Console. Vous devez utiliser le AWS Command Line Interface (AWS CLI) ou l'API. Pour de plus amples informations, veuillez consulter Configuration de la fonction Supprimer MFA.

À l'aide du AWS CLI

L'exemple suivant active le versionnement sur un compartiment S3 à usage général.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled
```

L'exemple suivant active la gestion des versions S3 et la fonction Supprimer l'authentification multifactorielle (MFA) sur un compartiment.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

> **Note**
>
> L'utilisation de la fonction Supprimer MFA nécessite un périphérique d'authentification physique ou virtuel approuvé. Pour en savoir plus sur l'utilisation de la fonction Supprimer MFA dans Amazon S3, consultez Configuration de la fonction Supprimer MFA.

Pour plus d'informations sur l'activation de la gestion des versions à l'aide du AWS CLI, consultez put-bucket-versioningla référence des AWS CLI commandes.

À l'aide du AWS SDKs

Les exemples suivants activent le contrôle de version sur un compartiment, puis récupèrent le statut de version à l'aide du AWS SDK pour Java et du. AWS SDK pour .NET Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez le AWS Developer Center.

.NET

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using System;
using Amazon.S3;
using Amazon.S3.Model;

namespace s3.amazon.com.docsamples
{
    class BucketVersioningConfiguration
    {
        static string bucketName = "*** bucket name ***";
```

```
        public static void Main(string[] args)
        {
            using (var client = new AmazonS3Client(Amazon.RegionEndpoint.USEast1))
            {
                try
                {
                    EnableVersioningOnBucket(client);
                    string bucketVersioningStatus =
RetrieveBucketVersioningConfiguration(client);
                }
                catch (AmazonS3Exception amazonS3Exception)
                {
                    if (amazonS3Exception.ErrorCode != null &&
                        (amazonS3Exception.ErrorCode.Equals("InvalidAccessKeyId")
                        ||
                        amazonS3Exception.ErrorCode.Equals("InvalidSecurity")))
                    {
                        Console.WriteLine("Check the provided AWS Credentials.");
                        Console.WriteLine(
                        "To sign up for service, go to http://aws.amazon.com/s3");
                    }
                    else
                    {
                        Console.WriteLine(
                         "Error occurred. Message:'{0}' when listing objects",
                         amazonS3Exception.Message);
                    }
                }
            }

            Console.WriteLine("Press any key to continue...");
            Console.ReadKey();
        }

        static void EnableVersioningOnBucket(IAmazonS3 client)
        {

                PutBucketVersioningRequest request = new PutBucketVersioningRequest
                {
                    BucketName = bucketName,
                    VersioningConfig = new S3BucketVersioningConfig
                    {
                        Status = VersionStatus.Enabled
```

```
                    }
                };

                PutBucketVersioningResponse response =
 client.PutBucketVersioning(request);
        }


        static string RetrieveBucketVersioningConfiguration(IAmazonS3 client)
        {
                GetBucketVersioningRequest request = new GetBucketVersioningRequest
                {
                    BucketName = bucketName
                };

                GetBucketVersioningResponse response =
 client.GetBucketVersioning(request);
                return response.VersioningConfig.Status;
            }
    }
}
```

Java

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, consultez Getting Started dans le guide du AWS SDK pour Java développeur.

```
import java.io.IOException;

import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Region;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3Client;
import com.amazonaws.services.s3.model.AmazonS3Exception;
import com.amazonaws.services.s3.model.BucketVersioningConfiguration;
import com.amazonaws.services.s3.model.SetBucketVersioningConfigurationRequest;

public class BucketVersioningConfigurationExample {
    public static String bucketName = "*** bucket name ***";
    public static AmazonS3Client s3Client;

    public static void main(String[] args) throws IOException {
        s3Client = new AmazonS3Client(new ProfileCredentialsProvider());
```

```
        s3Client.setRegion(Region.getRegion(Regions.US_EAST_1));
        try {

            // 1. Enable versioning on the bucket.
         BucketVersioningConfiguration configuration =
           new BucketVersioningConfiguration().withStatus("Enabled");

   SetBucketVersioningConfigurationRequest setBucketVersioningConfigurationRequest
 =
     new SetBucketVersioningConfigurationRequest(bucketName,configuration);


 s3Client.setBucketVersioningConfiguration(setBucketVersioningConfigurationRequest);

   // 2. Get bucket versioning configuration information.
   BucketVersioningConfiguration conf =
 s3Client.getBucketVersioningConfiguration(bucketName);
    System.out.println("bucket versioning configuration status:    " +
 conf.getStatus());

        } catch (AmazonS3Exception amazonS3Exception) {
            System.out.format("An Amazon S3 error occurred. Exception: %s",
 amazonS3Exception.toString());
        } catch (Exception ex) {
            System.out.format("Exception: %s", ex.toString());
        }
    }
}
```

Python

L'exemple de code Python suivant crée un compartiment Amazon S3, l'active pour la gestion des versions, et configure un cycle de vie qui fait expirer les versions d'objet anciennes après 7 jours.

```
def create_versioned_bucket(bucket_name, prefix):
    """
    Creates an Amazon S3 bucket, enables it for versioning, and configures a
 lifecycle
    that expires noncurrent object versions after 7 days.

    Adding a lifecycle configuration to a versioned bucket is a best practice.
    It helps prevent objects in the bucket from accumulating a large number of
    noncurrent versions, which can slow down request performance.
```

```
   Usage is shown in the usage_demo_single_object function at the end of this
module.

   :param bucket_name: The name of the bucket to create.
   :param prefix: Identifies which objects are automatically expired under the
                  configured lifecycle rules.
   :return: The newly created bucket.
   """
   try:
       bucket = s3.create_bucket(
           Bucket=bucket_name,
           CreateBucketConfiguration={
               "LocationConstraint": s3.meta.client.meta.region_name
           },
       )
       logger.info("Created bucket %s.", bucket.name)
   except ClientError as error:
       if error.response["Error"]["Code"] == "BucketAlreadyOwnedByYou":
           logger.warning("Bucket %s already exists! Using it.", bucket_name)
           bucket = s3.Bucket(bucket_name)
       else:
           logger.exception("Couldn't create bucket %s.", bucket_name)
           raise

   try:
       bucket.Versioning().enable()
       logger.info("Enabled versioning on bucket %s.", bucket.name)
   except ClientError:
       logger.exception("Couldn't enable versioning on bucket %s.", bucket.name)
       raise

   try:
       expiration = 7
       bucket.LifecycleConfiguration().put(
           LifecycleConfiguration={
               "Rules": [
                   {
                       "Status": "Enabled",
                       "Prefix": prefix,
                       "NoncurrentVersionExpiration": {"NoncurrentDays":
expiration},
                   }
               ]
```

```
                }
            )
            logger.info(
                "Configured lifecycle to expire noncurrent versions after %s days "
                "on bucket %s.",
                expiration,
                bucket.name,
            )
        except ClientError as error:
            logger.warning(
                "Couldn't configure lifecycle on bucket %s because %s. "
                "Continuing anyway.",
                bucket.name,
                error,
            )

        return bucket
```

Configuration de la fonction Supprimer MFA

Lorsque vous travaillez avec la gestion des versions S3 dans des compartiments Simple Storage Service (Amazon S3), vous pouvez ajouter une couche de sécurité en activant la fonction MFA delete (Suppression de l'authentification multifacteur). Quand vous procédez ainsi, le propriétaire du compartiment doit inclure deux formes d'authentification dans toute demande pour supprimer une version ou modifier l'état de la gestion des versions du compartiment.

La fonction Supprimer MFA exige une authentification supplémentaire pour les opérations suivantes :

- Changer l'état de la gestion des versions de votre compartiment
- Supprimer définitivement une version d'objet

La fonction Supprimer MFA exige deux formes d'authentification appliquées ensemble :

- Les informations d'identification de sécurité
- L'enchaînement d'un numéro de série valide, d'un espace et du code à six chiffres affiché sur un appareil d'authentification approuvé

La fonction Supprimer MFA fournit donc une sécurité supplémentaire, par exemple, en cas de mise en danger de vos informations d'identification de sécurité. La fonction Supprimer MFA peut aider à prévenir les suppressions accidentelles de compartiments en obligeant l'utilisateur qui lance l'action de suppression à prouver la possession physique d'un appareil MFA avec un code MFA et en ajoutant une couche de friction et de sécurité supplémentaire à l'action de suppression.

Pour identifier les compartiments pour lesquels la suppression MFA est activée, vous pouvez utiliser les métriques Amazon S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Pour plus d'informations, consultez Évaluer l'activité et l'utilisation de votre stockage avec S3 Storage Lens. Pour obtenir la liste complète des métriques, consultez le Glossaire des métriques S3 Storage Lens.

Le propriétaire du bucket, celui Compte AWS qui a créé le bucket (compte root) et tous les utilisateurs autorisés peuvent activer le versionnement. Toutefois, seul le propriétaire du compartiment (compte racine) peut activer la fonction Supprimer MFA. Pour plus d'informations, consultez la section Sécurisation de l'accès à AWS l'utilisation de la MFA sur le blog de AWS sécurité.

> **Note**
>
> Pour utiliser la suppression MFA avec la gestion des versions, vous devez activer `MFA Delete`. Toutefois, vous ne pouvez pas activer `MFA Delete` à l'aide de la AWS Management Console. Vous devez utiliser le AWS Command Line Interface (AWS CLI) ou l'API.
>
> Consultez la section Exemples dans la rubrique Activation de la gestion des versions sur les compartiments pour découvrir des cas d'utilisation de la suppression MFA avec la gestion des versions.
>
> Vous ne pouvez pas utiliser la suppression MFA avec des configurations de cycle de vie. Pour en savoir plus sur les configurations de cycle de vie et sur leur interaction avec d'autres configurations, consultez Comment le cycle de vie S3 interagit avec d'autres configurations de compartiments.

Pour activer ou désactiver la suppression MFA, vous devez utiliser la même API que celle utilisée pour configurer la gestion des versions sur un compartiment. Simple Storage Service (Amazon S3) stocke la configuration de la fonction Supprimer MFA dans la même sous-ressource de gestion des versions que celle de l'état de la gestion des versions du compartiment.

```
<VersioningConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Status>VersioningState</Status>
  <MfaDelete>MfaDeleteState</MfaDelete>
</VersioningConfiguration>
```

Pour utiliser la fonction Supprimer MFA, vous pouvez utiliser un appareil MFA matériel ou virtuel pour générer un code d'authentification. L'exemple suivant montre un code d'authentification généré et affiché sur un périphérique matériel.



Les fonctions Supprimer MFA et d'accès à l'API protégée par MFA sont conçues pour fournir une protection dans différents scénarios. Vous configurez la fonction Supprimer MFA sur un compartiment pour garantir que les données de votre compartiment ne puissent pas être supprimées par erreur. La fonction d'accès à l'API protégée par MFA est utilisée pour appliquer un autre facteur d'authentification (code MFA) lors de l'accès aux ressources Amazon S3 sensibles. Vous pouvez exiger que toute opération sur ces ressources Amazon S3 soit effectuée avec des informations d'identification temporaires créées grâce à la fonction MFA. Pour obtenir un exemple, consultez Exigence d'une MFA.

Pour en savoir plus sur l'achat et l'activation d'un appareil d'authentification, consultez Authentification multifactorielle.

Pour activer la gestion des versions S3 et configurer la fonction Supprimer MFA

À l'aide du AWS CLI

Le numéro de série est le numéro qui identifie de manière unique le dispositif MFA. Pour les dispositifs MFA physiques, il s'agit du numéro de série unique fourni avec le dispositif. Pour les dispositifs MFA virtuels, le numéro de série est l'ARN du dispositif.

L'exemple suivant active la gestion des versions S3 et la fonction Supprimer l'authentification multifactorielle (MFA) sur un compartiment.

```
aws s3api put-bucket-versioning --bucket amzn-s3-demo-bucket1 --versioning-
configuration Status=Enabled,MFADelete=Enabled --mfa "SERIAL 123456"
```

Utilisation de l'API REST

Pour plus d'informations sur la spécification de la suppression MFA à l'aide de l'API REST Amazon S3, consultez le manuel PutBucketVersioningAmazon Simple Storage Service API Reference.

Utiliser des objets dans un compartiment activé pour la gestion des versions

Les objets qui sont stockés dans un compartiment Simple Storage Service (Amazon S3) avant d'en définir l'état de la gestion des versions ont un ID de version `null`. Lorsque vous activez la gestion des versions, les objets existants dans le compartiment ne changent pas. Seule la façon dont Amazon S3 gère les objets dans les futures demandes change.

Transition des versions d'un objet

Vous pouvez définir les règles de configuration du cycle de vie pour les objets qui possèdent un cycle de vie bien défini, afin de transférer les versions d'objet vers la classe de stockage S3 Glacier Flexible Retrieval à un moment spécifique dans la durée de vie de l'objet. Pour plus d'informations, consultez Gestion du cycle de vie des objets.

Les rubriques de cette section expliquent plusieurs opérations d'objet dans un compartiment activé pour la gestion des versions. Pour plus d'informations sur la gestion des versions, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

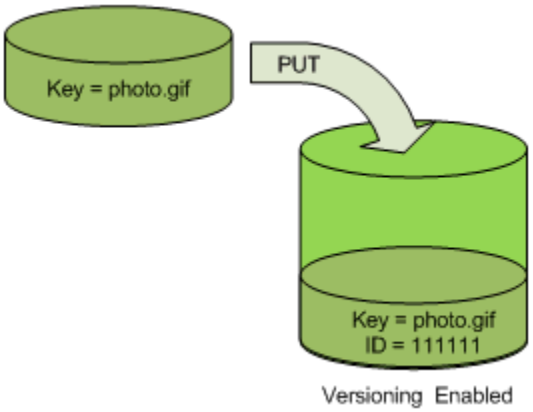
Rubriques

- Ajout d'objets dans des compartiments activés pour la gestion des versions
- Liste d'objets dans un compartiment activé pour la gestion des versions
- Récupération de versions d'objets à partir d'un compartiment activé pour la gestion des versions
- Suppression des versions d'objet d'un compartiment activé pour la gestion des versions
- Configuration des autorisations d'objet soumis à la gestion des versions

Ajout d'objets dans des compartiments activés pour la gestion des versions

Après avoir activé la gestion des versions sur un compartiment, Simple Storage Service (Amazon S3) ajoute automatiquement un ID de version unique à chaque objet stocké (à l'aide de `PUT`, `POST` ou `CopyObject`) dans le compartiment.

Le schéma suivant montre qu'Amazon S3 ajoute un ID de version unique à un objet ajouté à un compartiment activé pour la gestion des versions.



> **Note**
>
> Les valeurs de l'ID de version qu'Amazon S3 attribue sont sûres pour l'URL (elles peuvent être incluses dans une URI).

Pour plus d'informations sur la gestion des versions, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3. Vous pouvez ajouter des versions d'objets à un compartiment activé pour la gestion des versions à l'aide de la console et de l' AWS SDKsAPI REST.

Utilisation de la console

Pour obtenir des instructions, consultez Chargement d'objets.

À l'aide du AWS SDKs

Pour des exemples de téléchargement d'objets à l'aide AWS SDKs de Java, .NET et PHP, consultezChargement d'objets. Les exemples de chargement d'objets dans des compartiments non versionnés et activés pour la gestion des versions sont identiques, même si dans le cas des compartiments activés pour la gestion des versions, Amazon S3 attribue un numéro de version. Sinon, le numéro de version est null.

Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez le AWS Developer Center.

Utilisation de l'API REST

Pour ajouter des objets dans des compartiments activés pour la gestion des versions

1. Activez la gestion des versions sur un compartiment grâce à une demande `PutBucketVersioning`.

Pour plus d'informations, consultez PutBucketVersioning dans la Référence d'API Amazon Simple Storage Service.

2. Envoyez une demande `PUT`, `POST`, ou `CopyObject` pour stocker un objet dans le compartiment.

Lorsque vous ajoutez un objet dans un compartiment activé pour la gestion des versions, Simple Storage Service (Amazon S3) renvoie l'ID de version de l'objet dans l'en-tête de la réponse `x-amz-version-id`, comme illustré dans l'exemple suivant :

```
x-amz-version-id: 3/L4kqtJlcpXroDTDmJ+rmSpXd3dIbrHY
```

Liste d'objets dans un compartiment activé pour la gestion des versions

Cette section fournit des exemples de listes de versions d'objet à partir d'un compartiment activé pour la gestion des versions. Amazon S3 stocke les informations relatives aux versions d'objet dans la sous-ressource versions associée au compartiment. Pour plus d'informations, consultez Options de configuration des buckets à usage général. Pour répertorier les objets d'un compartiment dont la gestion des versions est activée, vous avez besoin de l'autorisation `ListBucketVersions`.

Utilisation de la console S3

Procédez comme suit pour utiliser la console Amazon S3 pour afficher les différentes versions d'un objet.

Pour afficher différentes versions d'un objet

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom du compartiment qui contient l'objet.
3. Pour afficher la liste des versions des objets du compartiment, choisissez le commutateur Show versions (Afficher les versions).

   Pour chaque version d'objet, la console affiche un ID de version unique, la date et l'heure auxquelles la version d'objet a été créée, et d'autres propriétés. (Les objets stockés dans le compartiment avant la configuration de l'état de la gestion des versions possèdent un ID de version null.)

   Pour répertorier les objets sans les versions, choisissez le commutateur List versions (Répertorier les versions).

Vous pouvez également afficher, télécharger et supprimer les versions d'un objet dans le panneau de présentation de l'objet sur la console. Pour de plus amples informations, veuillez consulter Affichage des propriétés d'un objet dans la console Amazon S3.

> **Note**
>
> Pour accéder à des versions d'objets antérieures à 300 versions, vous devez utiliser la AWS CLI ou l'URL de l'objet.

> **Important**
>
> Vous pouvez annuler la suppression d'un objet uniquement si celui-ci a été supprimé en tant que version la plus récente (version actuelle). Vous ne pouvez pas restaurer une version précédente d'un objet supprimé. Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

À l'aide du AWS SDKs

Les exemples de cette section montrent comment récupérer une liste d'objets à partir d'un compartiment activé pour la gestion des versions. Chaque demande renvoie jusqu'à 1 000 versions, sauf si vous spécifiez un nombre inférieur. Si le compartiment contient plus de versions que cette limite, vous devez envoyer une série de demandes pour récupérer la liste de toutes les versions. Ce processus de renvoi des résultats dans des « pages » s'appelle pagination.

Pour illustrer le fonctionnement de la pagination, les exemples limitent chaque réponse à deux versions d'objet. Après avoir récupéré la première page de résultats, chaque exemple vérifie si la liste de versions a été tronquée. Si tel est le cas, l'exemple continue de récupérer les pages jusqu'à ce que toutes les versions aient été récupérées.

> **Note**
>
> Les exemples suivants fonctionnent également avec un compartiment qui n'est pas activé pour la gestion des versions ou pour des objets qui n'ont pas de versions individuelles. Dans ces cas de figure, Amazon S3 renvoie la liste d'objets avec l'ID de version `null`.

Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez le AWS Developer Center.

Java

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, voir Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListVersionsRequest;
import com.amazonaws.services.s3.model.S3VersionSummary;
import com.amazonaws.services.s3.model.VersionListing;

public class ListKeysVersioningEnabledBucket {

    public static void main(String[] args) {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Retrieve the list of versions. If the bucket contains more versions
            // than the specified maximum number of results, Amazon S3 returns
            // one page of results per request.
            ListVersionsRequest request = new ListVersionsRequest()
                    .withBucketName(bucketName)
                    .withMaxResults(2);
            VersionListing versionListing = s3Client.listVersions(request);
            int numVersions = 0, numPages = 0;
            while (true) {
                numPages++;
                for (S3VersionSummary objectSummary :
 versionListing.getVersionSummaries()) {
                    System.out.printf("Retrieved object %s, version %s\n",
                            objectSummary.getKey(),
                            objectSummary.getVersionId());
                    numVersions++;
```

```
                }
                // Check whether there are more pages of versions to retrieve. If
                // there are, retrieve them. Otherwise, exit the loop.
                if (versionListing.isTruncated()) {
                    versionListing =
 s3Client.listNextBatchOfVersions(versionListing);
                } else {
                    break;
                }
            }
            System.out.println(numVersions + " object versions retrieved in " +
 numPages + " pages");
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

.NET

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class ListObjectsVersioningEnabledBucketTest
    {
        static string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
```

```
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main(string[] args)
        {
            s3Client = new AmazonS3Client(bucketRegion);
            GetObjectListWithAllVersionsAsync().Wait();
        }

        static async Task GetObjectListWithAllVersionsAsync()
        {
            try
            {
                ListVersionsRequest request = new ListVersionsRequest()
                {
                    BucketName = bucketName,
                    // You can optionally specify key name prefix in the request
                    // if you want list of object versions of a specific object.

                    // For this example we limit response to return list of 2
versions.
                    MaxKeys = 2
                };
                do
                {
                    ListVersionsResponse response = await
s3Client.ListVersionsAsync(request);
                    // Process response.
                    foreach (S3ObjectVersion entry in response.Versions)
                    {
                        Console.WriteLine("key = {0} size = {1}",
                            entry.Key, entry.Size);
                    }

                    // If response is truncated, set the marker to get the next
                    // set of keys.
                    if (response.IsTruncated)
                    {
                        request.KeyMarker = response.NextKeyMarker;
                        request.VersionIdMarker = response.NextVersionIdMarker;
                    }
                    else
                    {
```

```
                    request = null;
                }
            } while (request != null);
        }
        catch (AmazonS3Exception e)
        {
            Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
        }
        catch (Exception e)
        {
            Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
        }
    }
}
```

Utilisation de l'API REST

Example — Liste de toutes les versions d'objet dans un compartiment

Pour répertorier toutes les versions de tous les objets d'un compartiment, vous utilisez la sous-ressource `versions` dans une demande `GET Bucket`. Amazon S3 peut récupérer 1 000 objets maximum, et chaque version d'objet compte pleinement comme un objet. Par conséquent, si un compartiment contient deux clés (par exemple, `photo.gif` et `picture.jpg`), et que la première clé comporte 990 versions et la seconde 400 versions, une seule demande peut récupérer les 990 versions de `photo.gif` et uniquement les 10 versions les plus récentes de `picture.jpg`.

Amazon S3 renvoie des versions d'objet dans l'ordre dans lequel elles sont stockées ; les plus récemment stockées sont renvoyées en premier.

Dans une demande `GET Bucket`, incluez la sous-ressource `versions`.

```
GET /?versions HTTP/1.1
Host: bucketName.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 +0000
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Example — Récupération de toutes les versions d'une clé

Pour récupérer un sous-ensemble de versions d'objet, vous utilisez les paramètres de requête pour `GET Bucket`. Pour de plus amples informations, veuillez consulter GET Bucket.

1. Configurez le paramètre `prefix` sur la clé de l'objet que vous souhaitez récupérer.
2. Envoyez une demande `GET Bucket` grâce à la sous-ressource `versions` et `prefix`.

   ```
   GET /?versions&prefix=objectName HTTP/1.1
   ```

Example — Récupération d'objets à l'aide d'un préfixe

L'exemple suivant récupère des objets dont la clé est ou commence par `myObject`.

```
GET /?versions&prefix=myObject HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Vous pouvez utiliser les autres paramètres de la demande pour récupérer un sous-ensemble de toutes les versions de l'objet. Pour plus d'informations, consultez GET Bucket dans la Référence d'API Amazon Simple Storage Service.

Example — Récupération d'une liste d'objets supplémentaires si la réponse est tronquée

Si le nombre d'objets qui peuvent être renvoyés dans une demande `GET` dépasse la valeur de `max-keys`, la réponse contient `<isTruncated>true</isTruncated>`, et inclut la première clé (dans `NextKeyMarker`) et le premier ID de version (dans `NextVersionIdMarker`) qui satisfont la demande, mais qui n'ont pas été renvoyés. Vous utilisez ces valeurs renvoyées comme la position de départ dans une demande suivante pour récupérer les objets supplémentaires qui satisfont la demande `GET`.

Utilisez le processus suivant pour récupérer des objets supplémentaires qui satisfont la demande `GET Bucket versions` originale à partir d'un compartiment. Pour plus d'informations sur `key-marker`, `version-id-marker`, `NextKeyMarker` et `NextVersionIdMarker`, consultez GET Bucket dans la référence de l'API Amazon Simple Storage Service.

Ces quelques réponses supplémentaires satisfont à la requête `GET` d'origine :

- Configurez la valeur de `key-marker` sur la clé renvoyée dans `NextKeyMarker` dans la réponse précédente.
- Configurez la valeur de `version-id-marker` sur l'ID de version renvoyé dans `NextVersionIdMarker` dans la réponse précédente.
- Envoyez une demande `GET Bucket versions` avec `key-marker` et `version-id-marker`.

Example — Récupération des objets commençant par une clé et un ID de version spécifiés

```
GET /?versions&key-marker=myObject&version-id-marker=298459348571 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

À l'aide du AWS CLI

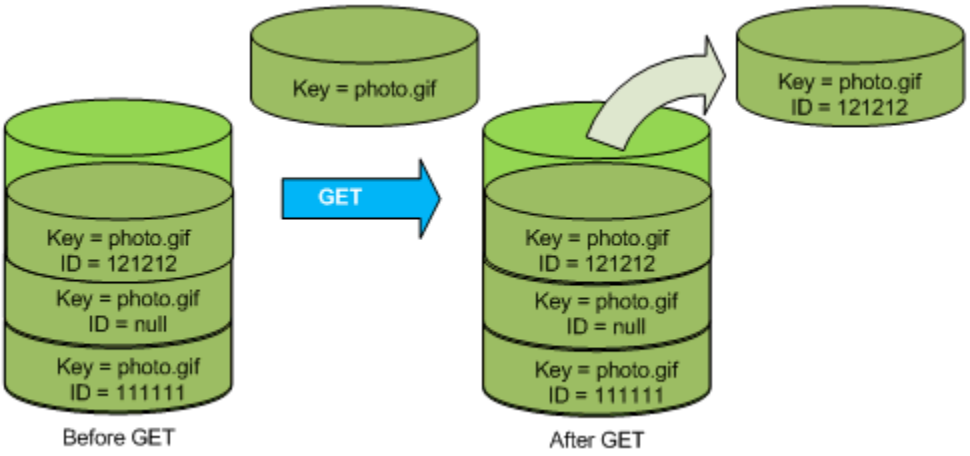
La commande suivante renvoie des métadonnées relatives à toutes les versions des objets contenus dans un compartiment.

```
aws s3api list-object-versions --bucket amzn-s3-demo-bucket1
```

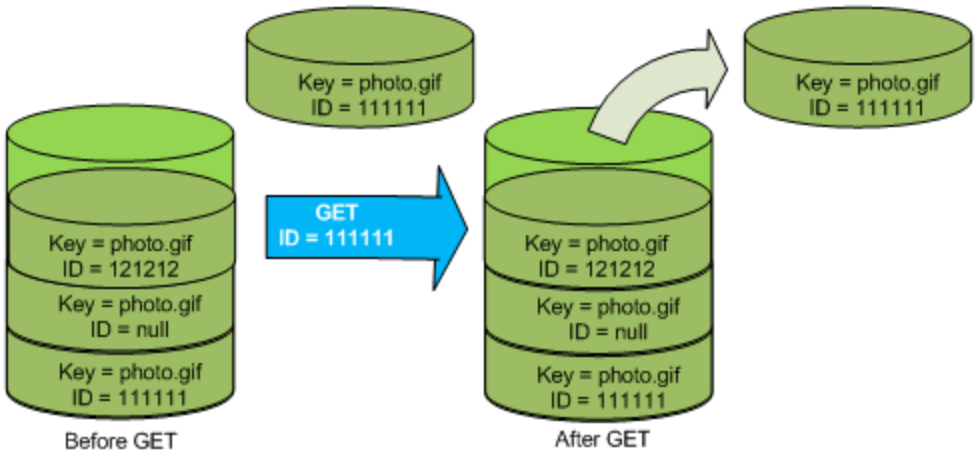
Pour plus d'informations sur `list-object-versions`, consultez list-object-versions dans la Référence des commandes de l'AWS CLI .

Récupération de versions d'objets à partir d'un compartiment activé pour la gestion des versions

La gestion des versions dans Simple Storage Service (Amazon S3) est un moyen de conserver plusieurs variantes d'un objet dans le même compartiment. Une simple demande `GET` récupère la version actuelle d'un objet. Le schéma suivant montre comment une demande `GET` renvoie la version actuelle de l'objet, `photo.gif`.



Pour récupérer une version spécifique, vous devez spécifier son ID de version. Le schéma suivant montre qu'une demande `GET versionId` récupère la version spécifiée de l'objet (pas nécessairement la version actuelle).



Vous pouvez récupérer des versions d'objets dans Amazon S3 à l'aide de la console ou de l'API REST. AWS SDKs

> **Note**
>
> Pour accéder à des versions d'objets antérieures à 300 versions, vous devez utiliser la AWS CLI ou l'URL de l'objet.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom du compartiment qui contient l'objet.
3. Dans la liste Objets, choisissez le nom de l'objet.
4. Choisissez Versions.

   Amazon S3 affiche toutes les versions de l'objet.
5. Sélectionnez la case à cocher en regard de l'ID de version des versions que vous souhaitez récupérer.
6. Choisissez Actions, choisissez Téléchargeret enregistrez l'objet.

Vous pouvez également afficher, télécharger et supprimer les versions d'un objet dans le panneau de présentation de l'objet. Pour de plus amples informations, veuillez consulter Affichage des propriétés d'un objet dans la console Amazon S3.

> **Important**
>
> Vous pouvez annuler la suppression d'un objet uniquement si celui-ci a été supprimé en tant que version la plus récente (version actuelle). Vous ne pouvez pas restaurer une version précédente d'un objet supprimé. Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

À l'aide du AWS SDKs

Les exemples de chargement d'objets dans des compartiments non versionnés et activés pour la gestion des versions sont les mêmes. Toutefois, pour les compartiments activés pour la gestion des versions, Simple Storage Service (Amazon S3) attribue un numéro de version. Sinon, le numéro de version est null.

Pour des exemples de téléchargement d'objets à AWS SDKs l'aide de Java, .NET et PHP, consultez la section Téléchargement d'objets.

Pour des exemples de liste des versions d'objets utilisés AWS SDKs pour .NET et Rust, consultez Répertorier la version des objets dans un compartiment Amazon S3.

Utilisation de l'API REST

Pour récupérer une version d'objet spécifique

1. Configurez la valeur `versionId` sur l'ID de la version de l'objet que vous souhaitez récupérer.
2. Envoyez une demande `GET Object versionId`.

Example Récupération d'un objet soumis à la gestion des versions

La demande suivante récupère la version `L4kqtJlcpXroDTDmpUMLUo` de `my-image.jpg`.

```
GET /my-image.jpg?versionId=L4kqtJlcpXroDTDmpUMLUo HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Seules les métadonnées d'un objet peuvent être récupérées, et pas son contenu. Pour plus d'informations, consultez the section called "Récupération des métadonnées de version".

Pour plus d'informations sur la restauration d'une version d'objet précédente, consultez the section called "Restauration des versions précédentes".

Récupération des métadonnées d'une version d'objet

Si vous souhaitez uniquement récupérer les métadonnées d'un objet (et pas son contenu), vous utilisez l'opération `HEAD`. Par défaut, vous obtenez les métadonnées de la version la plus récente. Pour récupérer les métadonnées d'une version d'objet spécifique, vous spécifiez son ID de version.

Pour récupérer les métadonnées d'une version d'objet

1. Configurez la valeur `versionId` sur l'ID de la version de l'objet dont vous souhaitez récupérer les métadonnées.
2. Envoyez une demande `HEAD Object versionId`.

Example — Récupération des métadonnées d'un objet soumis à la gestion des versions

La requête suivante récupère les métadonnées de la version `3HL4kqCxf3vjVBH40Nrjfkd` de `my-image.jpg`.

```
HEAD /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Voici un exemple de réponse.

```
HTTP/1.1 200 OK
x-amz-id-2: ef8yU9AS1ed4OpIszj7UDNEHGran
x-amz-request-id: 318BC8BC143432E5
x-amz-version-id: 3HL4kqtJlcpXroDTDmjVBH40Nrjfkd
Date: Wed, 28 Oct 2009 22:32:00 GMT
Last-Modified: Sun, 1 Jan 2006 12:00:00 GMT
ETag: "fba9dede5f27731c9771645a39863328"
Content-Length: 434234
Content-Type: text/plain
Connection: close
Server: AmazonS3
```

Restauration des versions précédentes

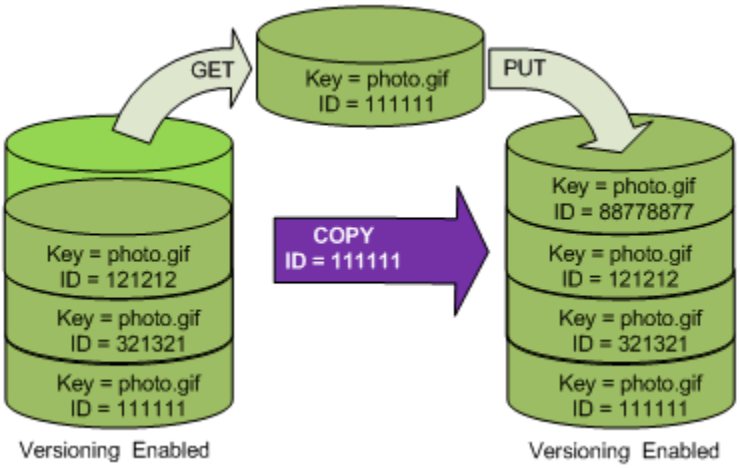
Vous pouvez utiliser la gestion des versions pour récupérer les versions précédentes d'un objet. Pour ce faire, deux approches sont possibles :

- La copie d'une version précédente de l'objet dans le même compartiment.

  L'objet copié devient la version actuelle de cet objet et toutes les versions d'objet sont préservées.
- La suppression définitive de la version actuelle de l'objet.

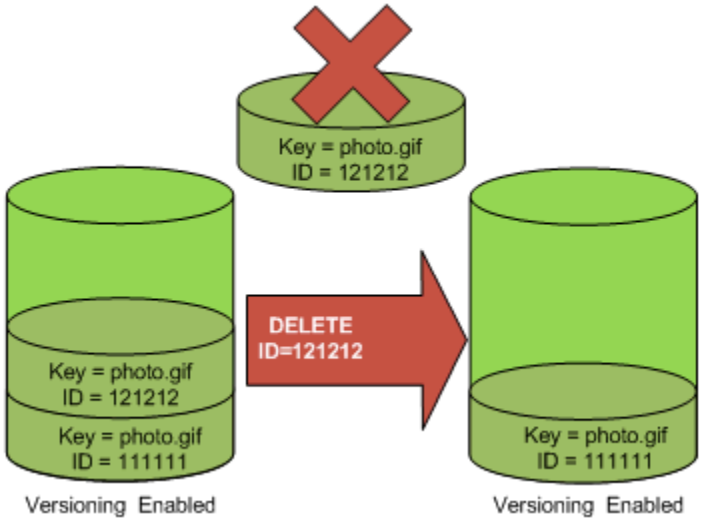
  Lorsque vous supprimez la version d'objet actuelle, vous transformez la version précédente en version actuelle de cet objet.

Etant donné que toutes les versions d'objet sont préservées, vous pouvez réaliser une version antérieure à la version actuelle en copiant une version spécifique de l'objet dans le même compartiment. Dans le schéma suivant, l'objet source (ID = 111111) est copié dans le même compartiment. Amazon S3 fournit un nouvel ID (88778877) qui devient la version actuelle de l'objet. Le compartiment possède donc la version d'objet originale (111111) et sa copie (88778877). Pour plus d'informations sur l'obtention d'une version précédente, puis son chargement pour en faire la version actuelle, consultez Récupération des versions d'objets à partir d'un compartiment activé pour la gestion des versions et Chargement d'objets.



Une version ultérieure GET récupère la version 88778877.

Le schéma suivant illustre comment la suppression de la version actuelle (121212) d'un objet permet à la version précédente (111111) de devenir l'objet actuel. Pour plus d'informations sur la suppression d'un objet, consultez Suppression d'un objet unique.



Une version ultérieure GET récupère la version 111111.

> **Note**
>
> Pour restaurer des versions d'objets par lots, vous pouvez utiliser l'opération `CopyObject`. L'opération `CopyObject` copie chaque objet spécifié dans le manifeste. Cependant, sachez que les objets ne sont pas nécessairement copiés dans le même ordre que celui dans lequel ils apparaissent dans le manifeste. Pour les compartiments activés pour la gestion des versions, si la préservation de l'ordre des versions actuelles ou anciennes est importante,

vous devez d'abord copier toutes les anciennes versions. Ensuite, une fois la première tâche terminée, copiez les versions actuelles dans une tâche ultérieure.

Pour restaurer les versions d'objets précédentes

Pour plus d'informations sur la restauration d'objets supprimés, consultez Comment puis-je récupérer un objet Amazon S3 qui a été supprimé dans un compartiment activé pour la gestion des versions ? dans le AWS re:Post Knowledge Center.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom du compartiment qui contient l'objet.
3. Dans la liste Objets, choisissez le nom de l'objet.
4. Choisissez Versions.

   Amazon S3 affiche toutes les versions de l'objet.
5. Sélectionnez la case à cocher en regard de l'ID de version des versions que vous souhaitez récupérer.
6. Choisissez Actions, choisissez Téléchargeret enregistrez l'objet.

Vous pouvez également afficher, télécharger et supprimer les versions d'un objet dans le panneau de présentation de l'objet. Pour de plus amples informations, veuillez consulter Affichage des propriétés d'un objet dans la console Amazon S3.

⚠ Important

Vous pouvez annuler la suppression d'un objet uniquement si celui-ci a été supprimé en tant que version la plus récente (version actuelle). Vous ne pouvez pas restaurer une version précédente d'un objet supprimé. Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

À l'aide du AWS SDKs

Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez le AWS Developer Center.

Python

L'exemple de code Python suivant restaure la version précédente d'un objet versionné en supprimant toutes les versions qui sont apparues après la version de restauration spécifiée.

```
def rollback_object(bucket, object_key, version_id):
    """
    Rolls back an object to an earlier version by deleting all versions that
    occurred after the specified rollback version.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that holds the object to roll back.
    :param object_key: The object to roll back.
    :param version_id: The version ID to roll back to.
    """
    # Versions must be sorted by last_modified date because delete markers are
    # at the end of the list even when they are interspersed in time.
    versions = sorted(
        bucket.object_versions.filter(Prefix=object_key),
        key=attrgetter("last_modified"),
        reverse=True,
    )

    logger.debug(
        "Got versions:\n%s",
        "\n".join(
            [
                f"\t{version.version_id}, last modified {version.last_modified}"
                for version in versions
            ]
        ),
    )

    if version_id in [ver.version_id for ver in versions]:
        print(f"Rolling back to version {version_id}")
        for version in versions:
            if version.version_id != version_id:
                version.delete()
                print(f"Deleted version {version.version_id}")
            else:
                break
```

```
        print(f"Active version is now {bucket.Object(object_key).version_id}")
    else:
        raise KeyError(
            f"{version_id} was not found in the list of versions for "
f"{object_key}."
        )
```

Suppression des versions d'objet d'un compartiment activé pour la gestion des versions

Vous pouvez supprimer des versions d'objets des compartiments Amazon S3 quand vous le souhaitez. Vous pouvez également définir des règles de configuration du cycle de vie pour les objets qui possèdent un cycle de vie bien défini pour demander à Amazon S3 d'expirer les versions d'objet actuelles ou de supprimer définitivement les anciennes versions d'objet. Lorsque la gestion des versions est activée ou suspendue pour un compartiment, les actions de la configuration du cycle de vie fonctionnent comme suit :

- L'action `Expiration` s'applique à la version actuelle de l'objet. Au lieu de supprimer la version actuelle de l'objet, Amazon S3 la conserve en tant que version ancienne en ajoutant un marqueur de suppression, qui devient ensuite la version actuelle.
- L'action `NoncurrentVersionExpiration` s'applique aux anciennes versions d'objet, et Amazon S3 les supprime définitivement. Vous ne pouvez pas récupérer définitivement les objets supprimés.

Pour plus d'informations sur le cycle de vie S3, consultez Gestion du cycle de vie des objets et Exemples de configurations du cycle de vie S3.

Pour connaître le nombre de versions actuelles et anciennes des objets de vos compartiments, vous pouvez utiliser les métriques Amazon S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Pour plus d'informations, consultez Using S3 Storage Lens to optimize your storage costs (Utilisation de S3 Storage Lens pour optimiser vos coûts de stockage). Pour obtenir la liste complète des métriques, consultez le Glossaire des métriques S3 Storage Lens.

> **Note**
>
> Les tarifs Amazon S3 normaux s'appliquent pour chaque version d'un objet stockée et transférée, y compris les versions non actuelles de l'objet. Pour plus d'informations, consultez Tarification Amazon S3.

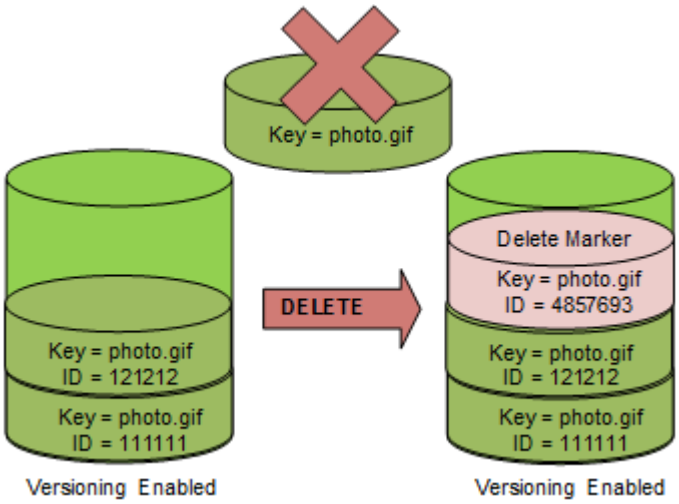
Supprimer les cas d'utilisation de demandes

Une demande `DELETE` possède les cas d'utilisation suivants :

- Lorsque la gestion des versions est activée, une simple demande `DELETE` ne peut pas supprimer définitivement un objet. (Une demande `DELETE` simple est une demande qui ne spécifie pas d'ID de version.) À la place, Amazon S3 insère un marqueur de suppression dans le compartiment qui devient la version actuelle de l'objet avec un nouvel ID.

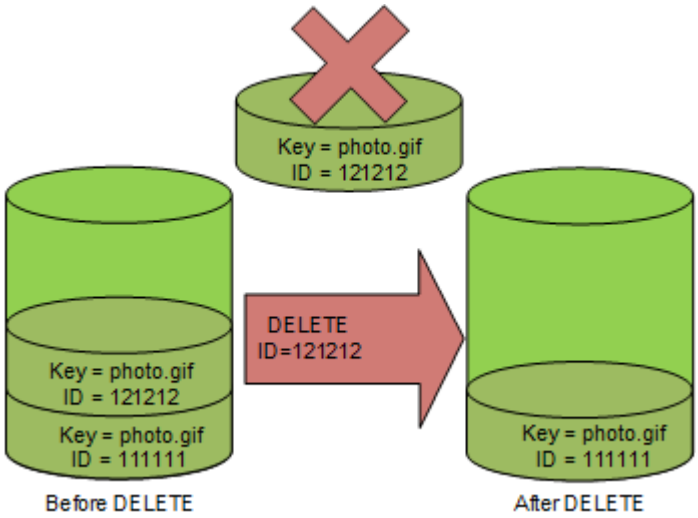
  Lorsque vous essayez de faire une demande `GET` sur un objet dont la version actuelle est un marqueur de suppression, Amazon S3 se comporte comme si l'objet avait été supprimé (même si ce n'est pas le cas) et renvoie une erreur 404. Pour plus d'informations, consultez Utilisation des marqueurs de suppression.

  Le schéma suivant montre qu'une simple demande `DELETE` ne supprime pas réellement l'objet spécifié. Au lieu de cela, Amazon S3 insère un marqueur de suppression.



- Pour supprimer définitivement les objets soumis à la gestion des versions, vous devez utiliser `DELETE Object versionId`.

  Le schéma suivant montre que la suppression d'un objet spécifié supprime définitivement cet objet.



Pour supprimer des versions d'un objet

Vous pouvez supprimer des versions d'objets dans Amazon S3 à l'aide de la console AWS SDKs, de l'API REST ou du AWS Command Line Interface.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom du compartiment qui contient l'objet.
3. Dans la liste Objets, choisissez le nom de l'objet.
4. Choisissez Versions.

   Amazon S3 affiche toutes les versions de l'objet.
5. Sélectionnez la case à cocher en regard de l'ID de version des versions que vous supprimer définitivement.
6. Choisissez Supprimer.
7. Dans Supprimer définitivement les objets ?, saisissez **`permanently delete`**.

> ⚠ Warning
>
> Lorsque vous supprimez définitivement une version d'objet, l'action ne peut pas être annulée.

8. Choisissez Supprimer les objets.

   Amazon S3 supprime la version de l'objet.

À l'aide du AWS SDKs

Pour des exemples de suppression d'objets à AWS SDKs l'aide de Java, .NET et PHP, consultezSuppression d'objets Amazon S3. Les exemples de suppression d'objets dans des compartiments non versionnés et activés pour la gestion des versions sont les mêmes. Toutefois, pour les compartiments activés pour la gestion des versions, Simple Storage Service (Amazon S3) attribue un numéro de version. Sinon, le numéro de version est null.

Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez le AWS Developer Center.

Python

L'exemple de code Python suivant supprime définitivement un objet assorti d'une gestion des versions en supprimant toutes ses versions.

```
def permanently_delete_object(bucket, object_key):
    """
    Permanently deletes a versioned object by deleting all of its versions.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to delete.
    """
    try:
        bucket.object_versions.filter(Prefix=object_key).delete()
        logger.info("Permanently deleted all versions of object %s.", object_key)
    except ClientError:
        logger.exception("Couldn't delete all versions of %s.", object_key)
        raise
```

Utilisation de l'API REST

Pour supprimer une version spécifique d'un objet

- Dans une demande `DELETE`, spécifiez un ID de version.

Example — Suppression d'une version spécifique

L'exemple suivant supprime la version `UIORUnfnd89493jJFJ` de `photo.gif`.

```
DELETE /photo.gif?versionId=UIORUnfnd89493jJFJ HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:xQE0diMbLRepdf3YB+FIEXAMPLE=
Content-Type: text/plain
Content-Length: 0
```

À l'aide du AWS CLI

La commande suivante supprime un objet nommé test.txt d'un compartiment nommé *amzn-s3-demo-bucket1*. Pour supprimer une version spécifique d'un objet, vous devez être le propriétaire du compartiment et vous devez utiliser la sous-ressource d'ID de version.

```
aws s3api delete-object --bucket amzn-s3-demo-bucket1 --key test.txt --version-
id versionID
```

Pour plus d'informations sur `delete-object`, consultez delete-object dans la Référence des commandes de l'AWS CLI .

Pour plus d'informations sur la suppression des versions d'objet, consultez ces rubriques :

- Utilisation des marqueurs de suppression
- Suppression des marqueurs de suppression pour rendre une version plus ancienne à jour
- Suppression d'un objet à partir d'un compartiment activé pour la fonction Supprimer MFA

Utilisation des marqueurs de suppression

Dans Amazon S3, un marqueur de suppression désigne un espace réservé (ou marqueur) pour un objet soumis à la gestion des versions qui a été spécifié dans une demande `DELETE` simple.

Une demande DELETE simple est une demande qui ne spécifie pas d'ID de version. Étant donné que l'objet était dans un compartiment activé pour la gestion des versions, il n'a pas été supprimé. Toutefois, à cause du marqueur de suppression, Amazon S3 se comporte comme si l'objet est supprimé. Vous pouvez utiliser un appel DELETE d'API Amazon S3 sur un marqueur de suppression. Pour ce faire, vous devez effectuer la DELETE demande en utilisant un utilisateur ou un rôle AWS Identity and Access Management (IAM) doté des autorisations appropriées.

Un marqueur de suppression possède un nom de clé (ou clé) et un ID de version comme tout autre objet. Toutefois, un marqueur de suppression diffère des autres objets des manières suivantes :

- Un marqueur de suppression n'a pas de données qui lui sont associées.
- Un marqueur de suppression n'est associé à aucune valeur de liste de contrôle d'accès (ACL).
- Si vous émettez une demande GET pour un marqueur de suppression, la demande GET ne récupère rien, car le marqueur de suppression ne contient aucune donnée. Plus précisément, lorsque votre demande GET ne spécifie pas de `versionId`, vous obtenez une erreur 404 (Introuvable).

Les marqueurs de suppression accumulent une charge minimale pour le stockage dans Amazon S3. La taille de stockage d'un marqueur de suppression est égale à la taille du nom de clé du marqueur de suppression. Un nom de clé est une séquence de caractères Unicode. L'encodage UTF-8 du nom de clé ajoute 1 à 4 octets de stockage à votre compartiment pour chaque caractère dans le nom. Les marqueurs de suppression sont stockés dans la classe de stockage S3 standard.

Si vous souhaitez connaître le nombre de marqueurs de suppression dont vous disposez et la classe de stockage dans laquelle ils sont stockés, vous pouvez utiliser Amazon S3 Storage Lens. Pour plus d'informations, consultez Évaluer l'activité et l'utilisation de votre stockage avec Amazon S3 Storage Lens et Glossaire des métriques Amazon S3 Storage Lens.

Pour en savoir plus sur les noms de clé, consultez Attribution d'un nom aux objets Amazon S3. Pour plus d'informations sur le marqueur de suppression, consultez Gestion des marqueurs de suppression.

Seul Simple Storage Service (Amazon S3) peut créer un marqueur de suppression, et il le fait dès que vous envoyez une demande `DeleteObject` sur un objet dans un compartiment activé ou désactivé pour la gestion des versions. L'objet spécifié dans la demande DELETE n'est pas réellement supprimé. A la place, le marqueur de suppression devient la version actuelle de l'objet. Le nom de clé de l'objet (ou clé) devient la clé du marqueur de suppression.

Quand vous obtenez un objet sans spécifier de `versionId` dans votre demande, si sa version actuelle est un marqueur de suppression, Amazon S3 fournit les réponses suivantes :

- Une erreur 404 (Introuvable)
- En-tête de réponse, `x-amz-delete-marker: true`

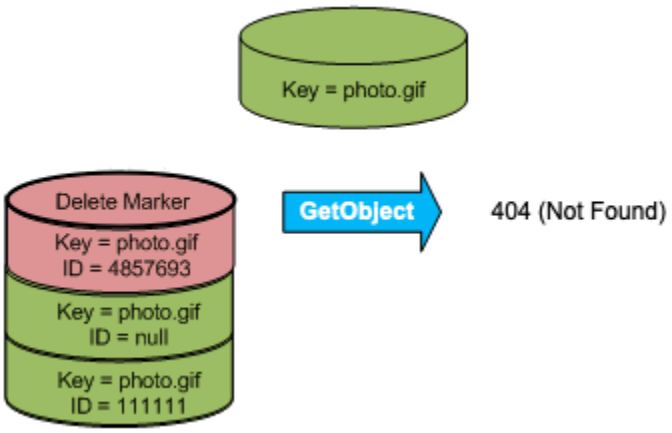
Quand vous obtenez un objet en spécifiant un `versionId` dans votre demande, si la version actuelle est un marqueur de suppression, Amazon S3 fournit les réponses suivantes :

- Une erreur 405 (méthode non autorisée)
- En-tête de réponse, `x-amz-delete-marker: true`
- Un en-tête de réponse `Last-Modified: timestamp` (uniquement lors de l'utilisation des opérations HeadObjectou de GetObjectl'API)

L'en-tête de réponse `x-amz-delete-marker: true` vous indique que l'objet consulté était un marqueur de suppression. Cet en-tête de réponse ne renvoie jamais `false`, car lorsque la valeur est `false`, la version actuelle ou spécifiée de l'objet n'est pas un marqueur de suppression.

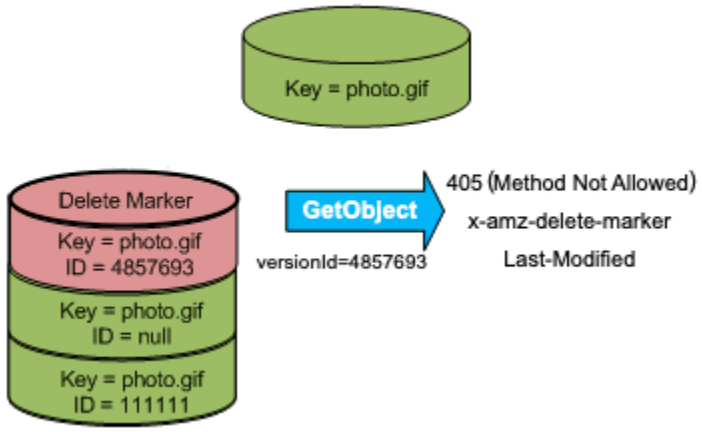
L'en-tête de réponse `Last-Modified` indique l'heure de création des marqueurs de suppression.

La figure suivante montre comment un appel d'API `GetObject` sur un objet dont la version actuelle est un marqueur de suppression répond avec une erreur 404 (Introuvable) et avec un en-tête de réponse incluant `x-amz-delete-marker: true`.



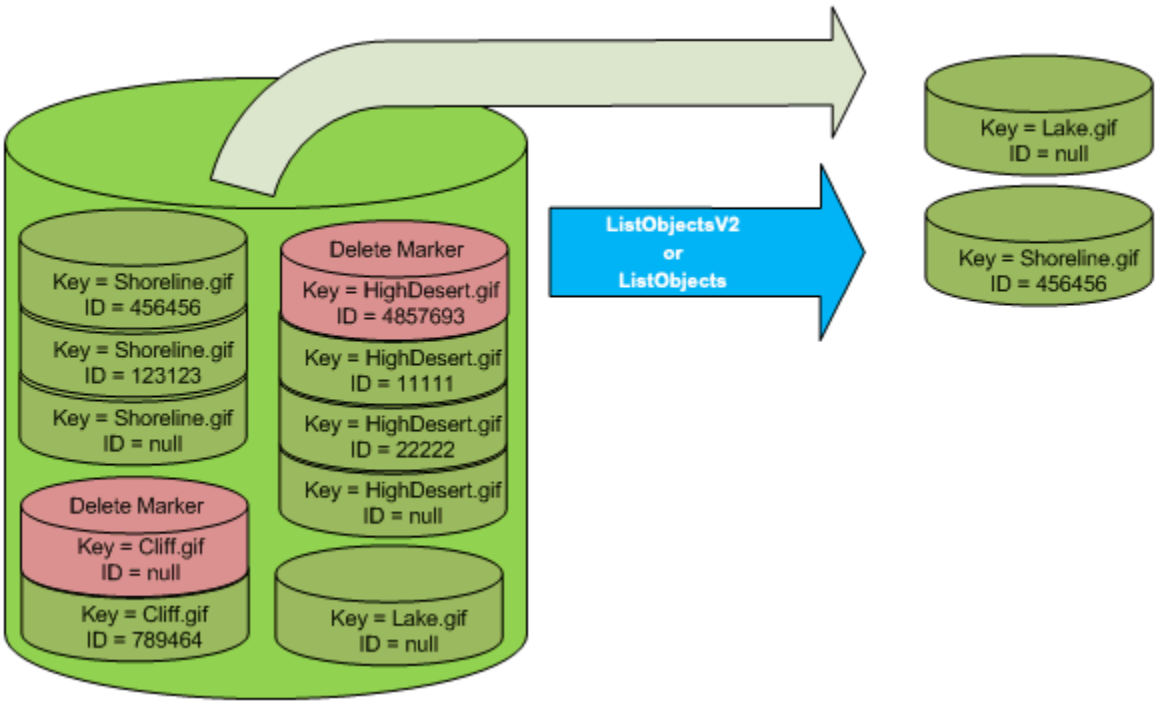
Si vous effectuez un appel `GetObject` sur un objet en spécifiant un `versionId` dans votre demande, et si la version spécifiée est un marqueur de suppression, Amazon S3 répond avec une

erreur 405 (Méthode non autorisée) et les en-têtes de réponse incluent `x-amz-delete-marker: true` et `Last-Modified: timestamp`.



Même s'ils sont remplacés, les marqueurs de suppression restent dans les versions de vos objets. La seule façon de répertorier les marqueurs de suppression (et les autres versions d'un objet) est d'utiliser une ListObjectVersionsrequête. Vous pouvez faire cette demande dans le en AWS Management Console répertoriant vos objets dans un compartiment à usage général et en sélectionnant Afficher les versions. Pour de plus amples informations, veuillez consulter Liste d'objets dans un compartiment activé pour la gestion des versions.

La figure suivante montre qu'une demande ListObjectsV2 ou ListObjects ne renvoie pas d'objets dont la version actuelle est un marqueur de suppression.



Gestion des marqueurs de suppression

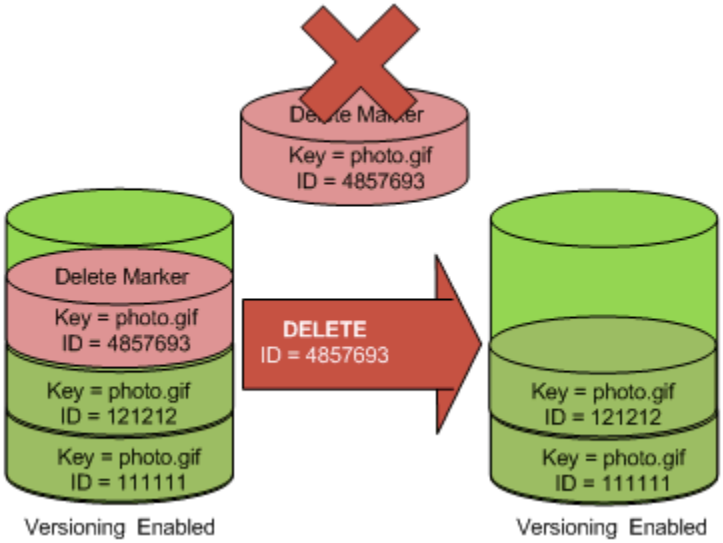
Configuration du cycle de vie pour nettoyer automatiquement les marqueurs de suppression expirés

Un marqueur de suppression d'objet expiré est un marqueur dans lequel toutes les versions d'objet sont supprimées et où il ne reste qu'un seul marqueur de suppression. Si la configuration de cycle de vie est définie pour supprimer les versions actuelles, ou si l'action `ExpiredObjectDeleteMarker` est explicitement définie, Amazon S3 supprime le marqueur de suppression de l'objet expiré. Pour obtenir un exemple, consultez Suppression des marqueurs de suppression des objets expirés dans un compartiment avec gestion des versions.

Suppression des marqueurs de suppression pour rendre une version plus ancienne à jour

Lorsque vous supprimez un objet d'un compartiment activé pour la gestion des versions, toutes les versions restent dans le compartiment et Simple Storage Service (Amazon S3) crée un marqueur de suppression pour l'objet. Pour annuler la suppression de l'objet, vous devez supprimer ce marqueur de suppression. Pour plus d'informations sur la gestion des versions et les marqueurs de suppression, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

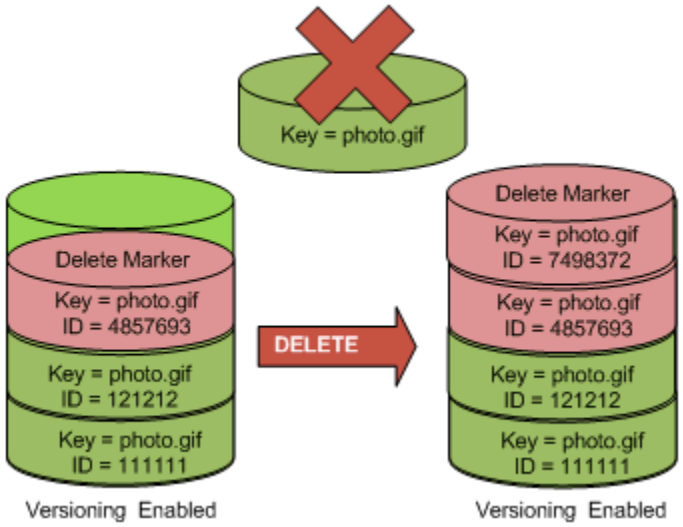
Pour supprimer un marqueur de suppression définitivement, vous devez inclure son ID de version dans une demande `DeleteObject versionId`. Le schéma suivant montre comment une demande `DeleteObject versionId` supprime définitivement un marqueur de suppression.



Suite à la suppression du marqueur de suppression, une simple demande `GET` récupère désormais l'ID de version actuelle (121212) de l'objet.

> **Note**
>
> Si vous utilisez une demande `DeleteObject` où la version actuelle est un marqueur de suppression (sans spécifier l'ID de version du marqueur de suppression), Amazon S3 ne supprime pas le marqueur de suppression, mais à la place, `PUT`s un autre marqueur de suppression.

Pour supprimer un marqueur de suppression avec un ID de version `NULL`, vous devez transmettre l'ID de version `NULL` comme ID de version dans la demande `DeleteObject`. La figure suivante illustre comment un demande `DeleteObject` adressée sans ID de version, où la version actuelle est un marqueur de suppression, ne supprime rien, mais ajoute à la place un marqueur de suppression supplémentaire avec un ID de version unique (7498372).



Utilisation de la console S3

Suivez ces étapes pour récupérer des objets supprimés qui ne sont pas des dossiers de votre compartiment S3, y compris les objets qui se trouvent dans ces dossiers.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Buckets (Compartiments), choisissez le nom du compartiment que vous souhaitez.
3. Pour afficher la liste des versions des objets du compartiment, choisissez le commutateur Répertorier les versions. Vous pourrez voir les marqueurs de suppression pour les objets supprimés.

4. Pour annuler la suppression d'un objet, vous devez supprimer le marqueur de suppression. Cochez la case en regard du marqueur de suppression de l'objet à récupérer, puis choisissez Delete (Supprimer).
5. Confirmez la suppression sur la page Delete objects (Supprimer les objets).

   a. Pour Permanently delete objects? (Supprimer définitivement des objets ?), saisissez **`permanently delete`**.

   b. Choisissez Supprimer les objets.

> **Note**
>
> Vous ne pouvez pas utiliser la console Amazon S3 pour restaurer des dossiers. Vous devez utiliser le AWS CLI ou le SDK. Pour des exemples, consultez Comment récupérer un objet Simple Storage Service (Amazon S3) supprimé d'un compartiment activé pour la gestion des versions ? dans le Centre de connaissances AWS .

Utilisation de l'API REST

Pour supprimer définitivement un marqueur de suppression

1. Configurez la valeur `versionId` sur l'ID de la version du marqueur de suppression que vous souhaitez supprimer.
2. Envoyez une demande `DELETE Object versionId`.

Example — Suppression d'un marqueur de suppression

L'exemple suivant supprime le marqueur de suppression pour la version 4857693 `photo.gif`.

```
DELETE /photo.gif?versionId=4857693 HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Lorsque vous supprimez un marqueur de suppression, Amazon S3 inclut les éléments suivants dans la réponse.

```
204 NoContent
```

```
x-amz-version-id: versionID
x-amz-delete-marker: true
```

À l'aide du AWS SDKs

Pour plus d'informations sur l'utilisation des autres AWS SDKs, consultez le AWS Developer Center.

Python

L'exemple de code Python suivant montre comment supprimer un marqueur de suppression d'un objet et transformer ainsi la version ancienne la plus récente en la version actuelle de l'objet.

```
def revive_object(bucket, object_key):
    """
    Revives a versioned object that was deleted by removing the object's active
    delete marker.
    A versioned object presents as deleted when its latest version is a delete
 marker.
    By removing the delete marker, we make the previous version the latest version
    and the object then presents as *not* deleted.

    Usage is shown in the usage_demo_single_object function at the end of this
 module.

    :param bucket: The bucket that contains the object.
    :param object_key: The object to revive.
    """
    # Get the latest version for the object.
    response = s3.meta.client.list_object_versions(
        Bucket=bucket.name, Prefix=object_key, MaxKeys=1
    )

    if "DeleteMarkers" in response:
        latest_version = response["DeleteMarkers"][0]
        if latest_version["IsLatest"]:
            logger.info(
                "Object %s was indeed deleted on %s. Let's revive it.",
                object_key,
                latest_version["LastModified"],
            )
            obj = bucket.Object(object_key)
            obj.Version(latest_version["VersionId"]).delete()
            logger.info(
```

```
                "Revived %s, active version is now %s  with body '%s'",
                object_key,
                obj.version_id,
                obj.get()["Body"].read(),
            )
        else:
            logger.warning(
                "Delete marker is not the latest version for %s!", object_key
            )
    elif "Versions" in response:
        logger.warning("Got an active version for %s, nothing to do.", object_key)
    else:
        logger.error("Couldn't get any version info for %s.", object_key)
```

Suppression d'un objet à partir d'un compartiment activé pour la fonction Supprimer MFA

Si la fonction Supprimer MFA est activée dans la configuration de la gestion des versions d'un compartiment, le propriétaire du compartiment doit inclure l'en-tête de la demande `x-amz-mfa` dans les demandes pour supprimer définitivement une version d'objet ou modifier l'état de la gestion des versions du compartiment. Les demandes qui incluent `x-amz-mfa` doivent utiliser HTTPS.

La valeur de l'en-tête est la concaténation du numéro de série du périphérique d'authentification, un espace et le code d'authentification affiché dessus. Si vous n'incluez pas cet en-tête de la demande, cette dernière échoue.

Pour en savoir plus sur les périphériques d'authentification, consultez Authentification multifacteur.

Example — Suppression d'un objet à partir d'un compartiment activé pour la fonction Supprimer MFA

L'exemple suivant montre comment supprimer `my-image.jpg` (avec la version spécifiée), qui se trouve dans un compartiment où la fonction Suppression MFA est activée.

Notez l'espace entre *`[SerialNumber]`* et*`[AuthenticationCode]`*. Pour plus d'informations, consultez DeleteObject dans la Référence d'API Amazon Simple Storage Service.

```
DELETE /my-image.jpg?versionId=3HL4kqCxf3vjVBH40Nrjfkd HTTPS/1.1
Host: bucketName.s3.amazonaws.com
x-amz-mfa: 20899872 301749
Date: Wed, 28 Oct 2009 22:32:00 GMT
```

```
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
```

Pour en savoir plus sur l'activation de la fonction Supprimer MFA, consultez Configuration de la fonction Supprimer MFA.

Configuration des autorisations d'objet soumis à la gestion des versions

Les autorisations pour les objets dans Amazon S3 sont définies au niveau de la version. Chaque version est dotée de son propre propriétaire d'objet. Celui Compte AWS qui crée la version de l'objet est le propriétaire. Vous pouvez donc configurer différentes autorisations pour différentes versions du même objet. Pour ce faire, vous devez spécifier l'ID de version de l'objet dont vous souhaitez configurer les autorisations dans une demande `PUT Object versionId acl`. Pour une description détaillée et des instructions d'utilisation ACLs, voirGestion des identités et des accès pour Amazon S3.

Example — Configuration des autorisations pour une version d'objet

La requête suivante définit les autorisations du bénéficiaire, `BucketOwner@amazon.com`, à `FULL_CONTROL` sur la clé, `my-image.jpg`, ID de version, `3HL4kqtJvjVBH40Nrjfkd`.

```
PUT /my-image.jpg?acl&versionId=3HL4kqtJvjVBH40Nrjfkd HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU=
Content-Length: 124

<AccessControlPolicy>
  <Owner>
    <ID>75cc57f09aa0c8caeab4f8c24e99d10f8e7faeebf76c078efc7c6caea54ba06a</ID>
    <DisplayName>mtd@amazon.com</DisplayName>
  </Owner>
  <AccessControlList>
    <Grant>
      <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:type="CanonicalUser">
        <ID>a9a7b886d6fd24a52fe8ca5bef65f89a64e0193f23000e241bf9b1c61be666e9</ID>
        <DisplayName>BucketOwner@amazon.com</DisplayName>
      </Grantee>
      <Permission>FULL_CONTROL</Permission>
    </Grant>
  </AccessControlList>
```

```
  </AccessControlPolicy>
```

De la même façon, pour obtenir les autorisations d'une version d'objet spécifique, vous devez spécifier son ID de version dans une demande `GET Object versionId acl`. Vous devez inclure l'ID de version car, par défaut, la demande `GET Object acl` renvoie les autorisations de la version actuelle de l'objet.

Example — Récupération des autorisations pour une version d'objet spécifique

Dans l'exemple suivant, Amazon S3 renvoie les autorisations pour la clé, `my-image.jpg`, l'ID de version, `DVBH40Nr8X8gUMLUo`.

```
GET /my-image.jpg?versionId=DVBH40Nr8X8gUMLUo&acl HTTP/1.1
Host: bucket.s3.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:0RQf4/cRonhpaBX5sCYVf1bNRuU
```

Pour plus d'informations, consultez GetObjectAcl dans la Référence d'API Amazon Simple Storage Service.

Utilisation des objets dans un compartiment désactivé pour la gestion des versions

Dans Simple Storage Service (Amazon S3), vous pouvez désactiver la gestion des versions pour stopper l'accumulation de nouvelles versions du même objet dans un compartiment. Vous pouvez le faire car vous ne souhaitez qu'une seule version d'un objet dans un compartiment. Ou, vous ne voudrez peut-être pas accumuler de frais pour plusieurs versions.

Lorsque vous désactivez la gestion des versions, les objets existants du compartiment ne changent pas. Seule la façon dont Amazon S3 gère les objets dans les futures demandes change. Les rubriques de cette section expliquent les diverses opérations d'objet dans un compartiment dont la gestion des versions est désactivée, notamment l'ajout, la récupération et la suppression des objets.

Pour plus d'informations sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3. Pour plus d'informations sur la récupération des versions d'objet, consultez Récupération de versions d'objets à partir d'un compartiment activé pour la gestion des versions.

Rubriques

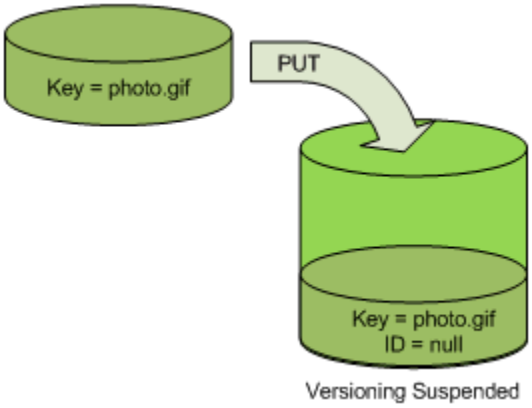
- Ajout d'objets dans des compartiments désactivés pour la gestion des versions
- Récupération d'objets à partir des compartiments désactivés pour la gestion des versions
- Suppression d'objets à partir des compartiments désactivés pour la gestion des versions

Ajout d'objets dans des compartiments désactivés pour la gestion des versions

Vous pouvez ajouter des objets aux compartiments désactivés pour la gestion des versions dans Simple Storage Service (Amazon S3) afin de créer l'objet avec un ID de version null ou bien pour écraser toute version d'objet avec un ID de version correspondant.

Après avoir désactivé la gestion des versions sur un compartiment, Simple Storage Service (Amazon S3) ajoute ensuite automatiquement un ID de version `null` à chaque objet stocké ultérieurement (à l'aide de la demande `PUT`, `POST`, ou `CopyObject`) dans le compartiment.

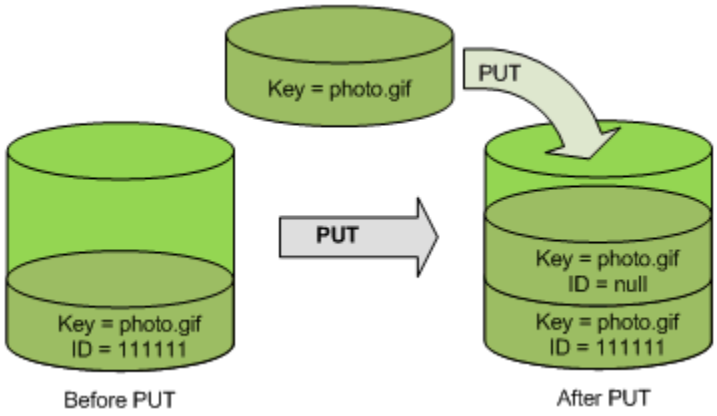
Le schéma suivant montre comment Amazon S3 ajoute l'ID de version `null` à un objet lorsqu'il est ajouté à un compartiment désactivé pour la gestion des versions.



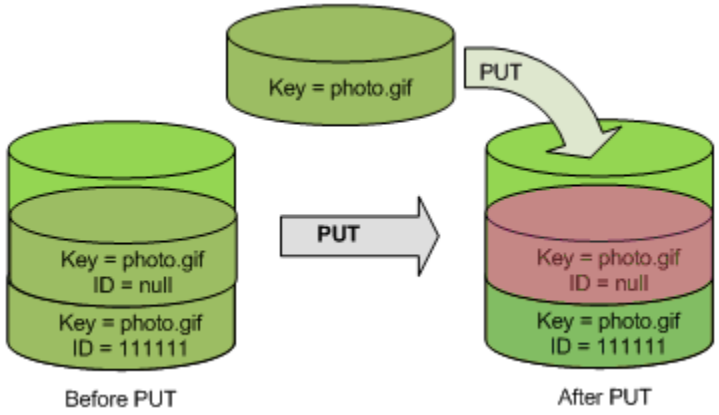
Si une version null est déjà dans le compartiment et que vous ajoutez un autre objet avec la même clé, l'objet ajouté remplace la version nulle originale.

En cas de présence d'objets versionnés dans le compartiment, la version pour laquelle vous faites une demande PUT devient la version actuelle de l'objet. Le schéma suivant montre en quoi l'ajout d'un objet à un compartiment qui contient des objets versionnés ne remplace pas l'objet déjà dans le compartiment.

Dans ce cas, la version 111111 était déjà dans le compartiment. Amazon S3 attache un ID de version null à l'objet en train d'être ajouté et le stocke dans le compartiment. La version 111111 n'est pas remplacée.



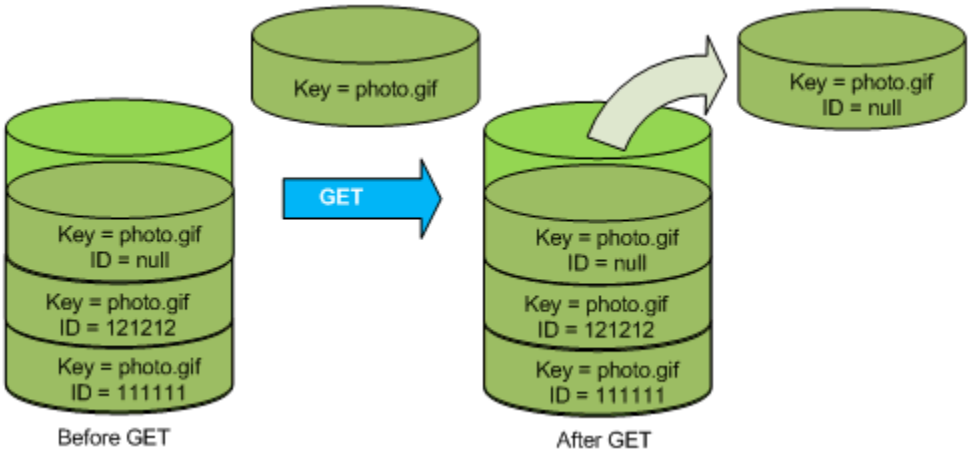
Si une version null existe déjà dans un compartiment, elle est remplacée, comme illustré dans le schéma suivant.



Notez que même si la clé et l'ID de version (`null`) de la version null sont identiques avant et après la demande PUT, le contenu de la version null initialement stocké dans le compartiment est remplacé par le contenu de l'objet PUT dans le compartiment.

Récupération d'objets à partir des compartiments désactivés pour la gestion des versions

Une demande `GET Object` renvoie la version actuelle d'un objet que vous ayez activé ou non la gestion des versions sur un compartiment. Le schéma suivant montre comment une simple demande GET renvoie la version actuelle d'un objet.



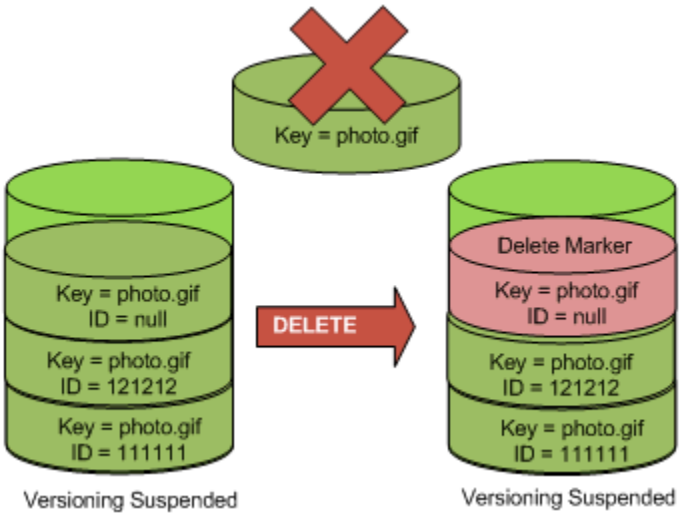
Suppression d'objets à partir des compartiments désactivés pour la gestion des versions

Vous pouvez supprimer des objets à partir des compartiments désactivés pour la gestion des versions afin de supprimer un objet ayant un ID de version null.

Si la gestion des versions est suspendue pour un compartiment, une demande `DELETE` :

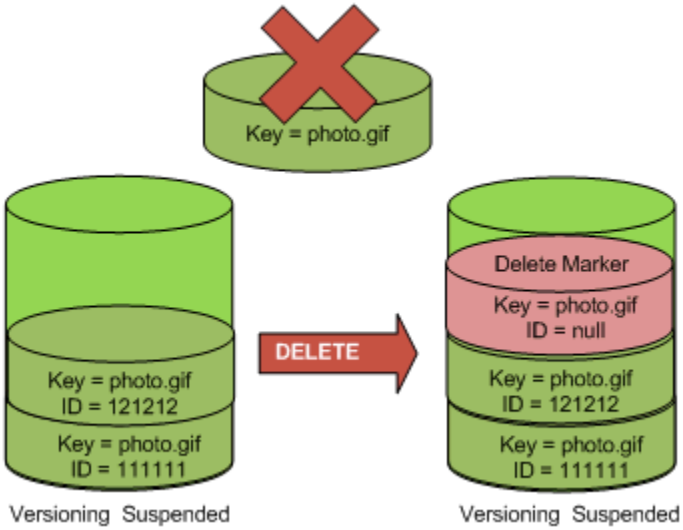
- Peut uniquement supprimer un objet dont l'ID de version est `null`.
- Ne supprime rien s'il n'y a aucune version null de l'objet dans le compartiment.
- Insère un marqueur de suppression dans le compartiment.

Si la gestion des versions du compartiment est suspendue, l'opération supprime l'objet dont la valeur `versionId` est null. Si un ID de version existe, Amazon S3 insère un marqueur de suppression qui devient la version actuelle de l'objet. La figure suivante montre comment une demande `DELETE` simple supprime une version null et Amazon S3 insère un marqueur de suppression à la place avec un ID de version `null`.

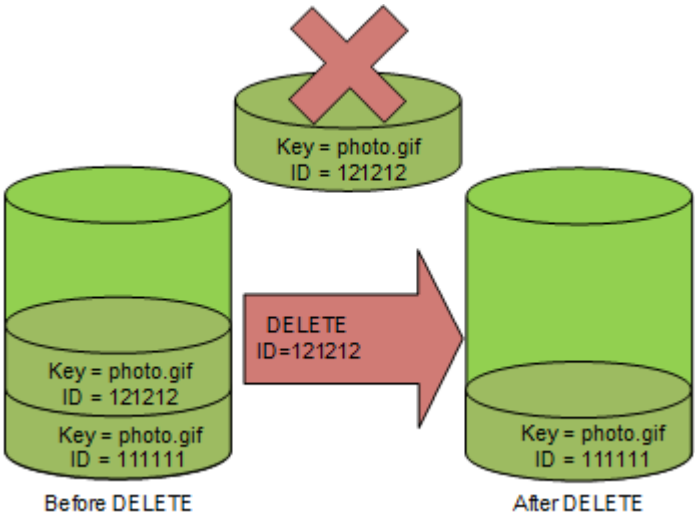


Pour supprimer définitivement un objet doté d'un `versionId`, vous devez inclure le `versionId` de l'objet dans la demande. Comme un marqueur de suppression ne contient aucun contenu, vous perdez le contenu pour la version `null` lorsqu'un marqueur de suppression la remplace.

Le schéma suivant montre un compartiment qui ne possède pas de version null. Dans ce cas, la commande `DELETE` ne supprime rien. À la place, Amazon S3 insère simplement un marqueur de suppression.



Même dans un compartiment dont la gestion des versions est suspendue, le propriétaire du compartiment peut supprimer définitivement une version spécifiée en incluant l'ID de la version dans la demande `DELETE`. Le schéma suivant montre que la suppression d'un objet spécifié supprime définitivement cette version de l'objet. Seul le propriétaire du compartiment peut supprimer une version d'objet spécifiée.



Résolution des problèmes de gestion des versions

Les rubriques suivantes peuvent vous aider à résoudre des problèmes courants de gestion des versions sur Amazon S3.

Rubriques

- Je souhaite récupérer des objets qui ont été supprimés accidentellement dans un compartiment avec la gestion des versions.
- Je souhaite supprimer définitivement les objets avec la gestion des versions
- Je constate une dégradation des performances après avoir activé la gestion des versions sur les compartiments

Je souhaite récupérer des objets qui ont été supprimés accidentellement dans un compartiment avec la gestion des versions.

En général, lorsque des versions d'objets sont supprimées des compartiments S3, Amazon S3 n'a aucun moyen de les récupérer. Toutefois, si vous avez activé la gestion des versions S3 sur votre compartiment S3, une demande `DELETE` qui ne spécifie pas d'ID de version ne peut pas supprimer définitivement un objet. Au lieu de cela, un marqueur de suppression est ajouté en tant qu'espace réservé. Ce marqueur de suppression devient la version actuelle de l'objet.

Pour vérifier si vos objets supprimés sont définitivement ou temporairement supprimés (avec un marqueur de suppression à leur place), procédez comme suit :

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment qui contient l'objet.
4. Dans la liste Objets, activez le bouton Afficher les versions à droite de la barre de recherche, puis recherchez l'objet supprimé dans la barre de recherche. Cette option n'est disponible que si la gestion des versions a précédemment été activée sur le compartiment.

   Vous pouvez également utiliser S3 Inventory pour rechercher des objets supprimés.
5. Si vous ne trouvez pas l'objet après avoir activé l'option Afficher les versions ou créé un rapport d'inventaire, et que vous ne trouvez pas non plus de marqueur de suppression de l'objet, la suppression est définitive et l'objet ne peut pas être récupéré.

Vous pouvez également vérifier le statut d'un objet supprimé à l'aide de l'opération `HeadObject` API depuis le AWS Command Line Interface (AWS CLI). Pour ce faire, utilisez la commande `head-object` suivante et remplacez *`user input placeholders`* par vos propres informations :

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html
```

Si vous exécutez la commande `head-object` sur un objet avec la gestion des versions dont la version actuelle est un marqueur de suppression, vous recevrez une erreur 404 Introuvable. Par exemple :

Une erreur s'est produite (404) lors de l'appel de l' HeadObject opération : Introuvable

Si vous exécutez la commande `head-object` sur un objet avec la gestion des versions et que vous fournissez l'ID de version de l'objet, Amazon S3 récupère les métadonnées de l'objet, confirmant ainsi que l'objet existe toujours et qu'il n'est pas supprimé définitivement.

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

```
{
"AcceptRanges": "bytes",
"ContentType": "text/html",
"LastModified": "Thu, 16 Apr 2015 18:19:14 GMT",
"ContentLength": 77,
"VersionId": "Zg5HyL7m.eZU9iM7AVlJkrqAiE.0UG4q",
"ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",
```

```
"Metadata": {}
}
```

Si l'objet est trouvé et que la version la plus récente est un marqueur de suppression, la version précédente de l'objet existe toujours. Le marqueur de suppression étant la version actuelle de l'objet, vous pouvez récupérer l'objet en supprimant le marqueur de suppression.

Une fois que vous avez supprimé définitivement le marqueur de suppression, la deuxième version la plus récente de l'objet devient la version actuelle de l'objet, ce qui rend votre objet à nouveau disponible. Pour une représentation visuelle de la façon dont les objets sont récupérés, consultez Suppression des marqueurs de suppression.

Pour supprimer une version spécifique d'un objet, vous devez être le propriétaire du compartiment. Pour supprimer un marqueur de suppression définitivement, vous devez inclure son ID de version dans une demande `DeleteObject`. Pour supprimer le marqueur de suppression, utilisez la commande suivante et remplacez *`user input placeholders`* par vos propres informations :

```
aws s3api delete-object --bucket amzn-s3-demo-bucket --key index.html --
version-id versionID
```

Pour plus d'informations sur la commande `delete-object`, consultez delete-object dans la Référence des commandes de l'AWS CLI . Pour plus d'informations sur la suppression permanente de marqueurs de suppression, consultez Gestion des marqueurs de suppression.

Je souhaite supprimer définitivement les objets avec la gestion des versions

Dans un compartiment avec la gestion des versions, une demande `DELETE` sans ID de version ne peut pas supprimer de façon permanente un objet. Au lieu de cela, une telle demande insère un marqueur de suppression.

Pour supprimer définitivement des objets avec la gestion des versions, vous pouvez choisir l'une des méthodes suivantes :

- Créez une règle de cycle de vie S3 pour supprimer définitivement les anciennes versions. Pour supprimer définitivement les versions anciennes d'objets, sous Supprimer définitivement les anciennes versions des objets, dans Jours après lesquels les objets deviennent anciens, saisissez le nombre de jours. Vous pouvez éventuellement spécifier le nombre de versions plus récentes à conserver en saisissant une valeur sous Number of newer versions to retain (Nombre de versions plus récentes à conserver). Pour plus d'informations sur la création de cette règle, consultez Setting an S3 Lifecycle configuration (Définition d'une configuration du cycle de vie S3).

- Supprimez une version spécifiée en incluant l'ID de version dans la demande DELETE. Pour plus d'informations, consultez How to delete versioned objects permanently (Comment supprimer des objets avec la gestion des versions de façon permanente).
- Créez une règle de cycle de vie pour faire expirer les versions actuelles. Pour faire expirer les versions actuelles des objets, sous Expirer les versions actuelles d'objets, dans Jours après la création de l'objet, saisissez le nombre de jours. Pour plus d'informations sur la création de cette règle de cycle de vie, consultez Setting an S3 Lifecycle configuration (Définition d'une configuration du cycle de vie S3).
- Pour supprimer définitivement tous les objets avec la gestion des versions et supprimer les marqueurs, créez deux règles de cycle de vie : l'une pour faire expirer les versions actuelles et supprimer définitivement les versions anciennes des objets, et l'autre pour supprimer les marqueurs de suppression d'objets expirés.

Dans un compartiment avec la gestion des versions, une demande DELETE qui ne spécifie pas d'ID de version ne peut supprimer que les objets dotés d'un identifiant de version NULL. Si l'objet a été chargé lorsque la gestion des versions était activée, une demande DELETE qui ne spécifie pas d'ID de version crée un marqueur de suppression de cet objet.

> **Note**
>
> Pour les compartiments avec le verrouillage des objets S3, une demande d'objet DELETE avec un ID de version d'objet protégé provoque une erreur 403 Accès refusé. Une demande d'objet DELETE sans ID de version ajoute un marqueur de suppression en tant que version la plus récente de l'objet avec une réponse 200 OK. Les objets protégés par le verrouillage des objets ne peuvent pas être supprimés définitivement tant que leurs périodes de rétention et leurs conservations légales ne sont pas levées. Pour plus d'informations, consultez the section called "Fonctionnement du verrouillage d'objets S3".

Je constate une dégradation des performances après avoir activé la gestion des versions sur les compartiments

Une dégradation des performances peut se produire sur les compartiments avec la gestion des versions s'il y a trop de marqueurs de suppression ou d'objets avec la gestion des versions et si les meilleures pratiques ne sont pas suivies.

Marqueurs de suppression trop nombreux

Après avoir activé la gestion des versions sur un compartiment, une demande DELETE faite à un objet sans ID de version crée un marqueur de suppression avec un ID de version unique. Les configurations de cycle de vie avec une règle Expirer les versions actuelles d'objets ajoutent un marqueur de suppression avec un ID de version unique à chaque objet. Un nombre excessif de marqueurs de suppression peut réduire les performances du compartiment.

Lorsque la gestion des versions est suspendue sur un compartiment, Amazon S3 marque l'ID de version comme NULL sur les nouveaux objets créés. Dans un compartiment avec la gestion des versions suspendue, l'action d'expiration entraîne la création par Amazon S3 d'un marqueur de suppression avec l'ID de version NULL. Dans un compartiment avec la gestion des versions suspendue, un marqueur de suppression NULL est créé pour chaque demande de suppression. Ces marqueurs de suppression NULL sont également appelés marqueurs de suppression d'objet expiré lorsque toutes les versions d'objet sont supprimées et qu'il ne reste qu'un seul marqueur de suppression. Si trop de marqueurs de suppression NULL s'accumulent, les performances du compartiment se dégradent.

Objets avec la gestion des versions trop nombreux

Si un compartiment avec la gestion des versions contient des objets contenant des millions de versions, le nombre d'erreurs 503 Service indisponible peut augmenter. Si vous remarquez une augmentation importante du nombre de réponses HTTP 503 Service indisponible reçues pour des demandes d'objet PUT ou DELETE vers un compartiment avec la gestion des versions, il est possible qu'un ou plusieurs objets du compartiment aient des millions de versions. Lorsque vous avez des objets avec des millions de versions, Amazon S3 limite automatiquement les demandes vers le compartiment. La limitation des demandes protège votre compartiment d'une quantité excessive de trafic de demandes qui pourrait potentiellement gêner d'autres demandes effectuées auprès du même compartiment.

Pour déterminer quels objets ont des millions de versions, utilisez S3 Inventory. S3 Inventory génère un rapport qui fournit une liste de fichiers plats des objets d'un compartiment. Pour plus d'informations, consultez Catalogage et analyse de vos données avec l'inventaire S3.

Pour vérifier si le compartiment contient un nombre élevé d'objets avec la gestion des versions, utilisez les métriques de S3 Storage Lens pour afficher Nombre d'objets de version actuelle Nombre d'objets de version ancienne et Nombre d'objets marqueur de suppression. Pour plus d'informations sur les métriques de Storage Lens, consultez Glossaire des métriques Amazon S3 Storage Lens.

L'équipe Amazon S3 encourage les clients à examiner les applications qui remplacent souvent le même objet et créent potentiellement des millions de versions de cet objet, afin de déterminer si

l'application fonctionne comme prévu. Par exemple, une application qui remplace le même objet toutes les minutes pendant une semaine peut créer plus de dix mille versions. Nous recommandons de stocker moins de cent mille versions pour chaque objet. Si votre cas d'utilisation nécessite des millions de versions pour un ou plusieurs objets, contactez l' AWS Support équipe pour obtenir de l'aide afin de déterminer la meilleure solution.

Bonnes pratiques

Pour éviter les problèmes de dégradation des performances liés à la gestion des versions, nous vous recommandons de suivre les bonnes pratiques suivantes :

- Activez une règle de cycle de vie pour faire expirer les anciennes versions des objets. Par exemple, vous pouvez créer une règle de cycle de vie pour faire expirer les versions anciennes 30 jours après la fin de la période d'inactivité de l'objet. Vous pouvez également conserver plusieurs anciennes versions si vous ne souhaitez pas toutes les supprimer. Pour plus d'informations, consultez Setting an S3 Lifecycle configuration (Définition d'une configuration du cycle de vie S3).
- Activez une règle de cycle de vie pour supprimer les marqueurs de suppression d'objets expirés auxquels aucun objet de données n'est associé dans le compartiment. Pour plus d'informations, consultez Suppression des marqueurs de suppression d'objet expiré.

Pour en savoir plus sur les bonnes pratiques d'optimisation des performances d'Amazon S3, consultez Schémas de conception des bonnes pratiques.

Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet

Le verrouillage d'objet S3 permet d'empêcher la suppression ou le remplacement d'objets Amazon S3 sur une période déterminée ou indéfinie. Object Lock utilise un modèle write-once-read-many(WORM) pour stocker des objets. Le verrouillage d'objet vous permet de satisfaire aux exigences réglementaires qui nécessitent le stockage WORM, ou bien d'ajouter une couche de protection supplémentaire contre la suppression et les modifications d'objets.

> **Note**
>
> Le verrouillage d'objet S3 a été évalué par Cohasset Associates en vue de son utilisation dans les environnements soumis aux réglementations SEC 17a-4, CFTC et FINRA. Pour

plus d'informations sur la conformité du verrouillage d'objet vis-à-vis de ces réglementations, consultez Cohasset Associates Compliance Assessment.

Le verrouillage d'objet propose deux façons de gérer la rétention des objets : les périodes de rétention et les conservations légales. Une version d'un objet peut être assortie d'une période de rétention, d'une conservation légale ou des deux.

- Période de conservation : une période de rétention indique une période fixe pendant laquelle une version d'objet reste verrouillée. Vous pouvez définir une période de conservation unique pour des objets individuels. En outre, vous pouvez définir une période de conservation par défaut sur un compartiment S3. Vous pouvez également limiter les périodes de conservation autorisées minimale et maximale en utilisant la clé de condition `s3:object-lock-remaining-retention-days` figurant dans la politique de compartiment. Cela vous permet d'établir une plage de périodes de conservation et de restreindre les périodes de conservation plus courtes ou plus longues que cette plage.
- Conservation légale : une conservation légale assure la même protection que la période de rétention, mais n'a pas de date d'expiration. La conservation légale reste en vigueur tant que vous ne la retirez pas explicitement. Les conservations légales sont indépendantes des périodes de rétention et sont mises en place sur des versions d'objet individuelles.

Le verrouillage d'objet fonctionne uniquement dans les compartiments pour lesquels la gestion des versions S3 est activée. Lorsque vous verrouillez une version d'objet, Amazon S3 stocke les informations de verrouillage dans les métadonnées de cette version d'objet. Le fait de définir une période de rétention ou une conservation légale sur un objet a pour effet de protéger uniquement la version spécifiée dans la demande. Les périodes de rétention et les conservation légales n'empêchent pas la création de nouvelles versions de l'objet, ni l'ajout de marqueurs de suppression sur l'objet. Pour en savoir plus sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Si vous placez un objet dans un compartiment qui contient déjà un objet protégé existant doté du même nom de clé d'objet, Amazon S3 crée une nouvelle version de cet objet. La version protégée existante de l'objet reste verrouillée conformément à sa configuration de rétention.

Fonctionnement du verrouillage d'objets S3

Rubriques

- Périodes de rétention
- Modes de conservation
- Conservations légales
- Bonnes pratiques pour l'utilisation du verrouillage d'objet S3
- Autorisations requises

Périodes de rétention

Une période de rétention protège une version d'objet pendant une durée fixe. Lorsque vous mettez en place une période de rétention sur une version d'objet, Amazon S3 stocke un horodatage dans les métadonnées de la version d'objet pour indiquer la date à laquelle la période de rétention expire. Après l'expiration de la période de rétention, la version de l'objet peut être remplacée ou supprimée.

Vous pouvez définir une période de rétention de manière explicite sur une version d'objet individuelle ou sur les propriétés d'un compartiment afin qu'elle s'applique automatiquement à tous les objets du compartiment. Lorsque vous appliquez explicitement une période de rétention à une version d'objet, vous spécifiez une Date de fin de conservation pour la version de l'objet. Amazon S3 stocke cette date dans les métadonnées de la version de l'objet.

Vous pouvez également définir une période de rétention dans les propriétés d'un compartiment. Lorsque vous définissez une période de rétention sur un compartiment, vous spécifiez une durée, en jours ou en années, pendant laquelle chaque version d'objet placée dans le compartiment sera protégée. Lorsque vous placez un objet dans le compartiment, Amazon S3 calcule une échéance de rétention pour la version de l'objet en ajoutant la durée spécifiée à l'horodatage de création de la version de l'objet. La version de l'objet est ensuite protégée exactement comme si vous aviez mis en place un verrouillage individuel de manière explicite avec la même période de rétention sur la version de l'objet.

> **Note**
>
> Lorsque vous placez (PUT) une version d'objet dotée d'un mode et d'une période de rétention individuels explicites dans un compartiment, les paramètres individuels de verrouillage d'objet de la version de l'objet remplacent tous les paramètres de rétention des propriétés du compartiment.

À l'instar de tous les autres paramètres de la fonctionnalité de verrouillage des objets, les périodes de rétention s'appliquent aux versions d'objet individuelles. Les différentes versions d'un seul objet peuvent avoir des modes et des périodes de rétention différents.

Par exemple, supposons que vous ayez un objet qui en est à 15 jours sur une période de conservation de 30 jours, et que vous PUT un objet dans Amazon S3 ayant le même nom et une période de rétention de 60 jours. Dans ce cas, votre demande PUT aboutit et Amazon S3 crée une nouvelle version de l'objet avec une période de rétention de 60 jours. L'ancienne version conservera sa période de rétention originale et pourra être supprimée dans 15 jours.

Après avoir appliqué un paramètre de rétention à une version d'objet, vous pouvez prolonger la période de rétention. Pour ce faire, envoyez une nouvelle demande de verrouillage d'objet pour la version d'objet avec une échéance de rétention postérieure à celle actuellement configurée pour la version d'objet. Amazon S3 remplace la période de rétention existante par la nouvelle période plus longue. Tout utilisateur disposant d'autorisations pour définir une période de rétention d'objet peut prolonger cette période pour une version d'objet. Pour définir une période de rétention, vous devez avoir l'autorisation `s3:PutObjectRetention`.

Lorsque vous définissez une période de rétention sur un objet ou un compartiment S3, vous devez sélectionner l'un des deux modes de rétention : conformité ou gouvernance.

Modes de conservation

Le verrouillage d'objet S3 fournit deux modes de rétention qui appliquent différents niveaux de protection à vos objets :

- Mode conformité
- Mode gouvernance

En mode Conformité, une version d'objet protégée ne peut pas être remplacée ou supprimée par n'importe quel utilisateur, notamment l'utilisateur racine de votre Compte AWS. Lorsqu'un objet est verrouillé en mode Conformité, son mode de rétention ne pas être modifié et sa période de rétention ne peut pas être raccourcie. Le mode Conformité garantit qu'une version d'objet ne peut pas être écrasée ou supprimée pendant la durée de la période de rétention.

> **Note**
>
> Le seul moyen de supprimer un objet en mode de conformité avant l'expiration de sa date de conservation est de supprimer l'objet associé Compte AWS.

Dans le mode Gouvernance, les utilisateurs ne peuvent pas remplacer ou supprimer une version d'objet ou en modifier les paramètres de verrouillage, sauf s'ils disposent d'autorisations spéciales. Avec le mode de gouvernance, vous protégez les objets contre leur suppression par la plupart des utilisateurs, mais vous pouvez toujours accorder à certains utilisateurs l'autorisation de modifier les paramètres de rétention ou de supprimer les objets si nécessaire. Vous pouvez également utiliser le mode Gouvernance pour tester les paramètres de la période de rétention, avant de créer une période de rétention en mode Conformité.

Pour remplacer ou supprimer des paramètres de rétention en mode de gouvernance, vous devez disposer de l'autorisation `s3:BypassGovernanceRetention` et explicitement inclure `x-amz-bypass-governance-retention:true` en tant qu'en-tête de toute demande nécessitant un remplacement dans le mode de gouvernance.

> **Note**
>
> Par défaut, la console Amazon S3 inclut l'en-tête `x-amz-bypass-governance-retention:true`. Si vous tentez de supprimer des objets protégés par le mode de gouvernance et que vous disposez de l'autorisation `s3:BypassGovernanceRetention`, l'opération aboutit.

Conservations légales

Avec le verrouillage d'objet, vous pouvez également définir une conservation légale sur une version d'objet. À l'instar d'une période de rétention, une conservation légale empêche une version d'objet d'être remplacée ou supprimée. Toutefois, une conservation légale n'a pas de période de rétention associée et reste en vigueur jusqu'à sa suppression. Les conservations légales peuvent être librement mises en place et supprimées par tous les utilisateurs disposant de l'autorisation `s3:PutObjectLegalHold`.

Les conservations légales sont indépendantes des périodes de rétention. La mise en place d'une conservation légale sur une version d'objet n'affecte pas le mode ou la période de rétention pour cette version d'objet.

Par exemple, supposons que vous définissiez une conservation légale sur une version d'objet, alors que cette version d'objet est également protégée par une période de rétention. Si la période de rétention expire, l'objet ne perd pas sa protection WORM. À la place, la conservation légale continue de protéger l'objet jusqu'à ce qu'un utilisateur autorisé la supprime de manière explicite. De la même façon, si vous supprimez une conservation légale alors qu'une période de rétention est en vigueur pour une version d'objet, cette dernière reste protégée jusqu'à l'expiration de la période de rétention.

Bonnes pratiques pour l'utilisation du verrouillage d'objet S3

Envisagez d'utiliser le Mode de gouvernance si vous souhaitez empêcher la suppression d'objets par la plupart des utilisateurs pendant une période de conservation prédéfinie, tout en permettant à certains utilisateurs disposant d'autorisations spéciales de modifier les paramètres de conservation ou de supprimer les objets.

Envisagez d'utiliser le Mode de conformité si vous ne voulez pas qu'un utilisateur, y compris l'utilisateur racine de votre Compte AWS, puisse supprimer les objets pendant une période de conservation prédéfinie. Vous pouvez utiliser ce mode au cas où vous auriez besoin de stocker des données conformes.

Vous pouvez utiliser la Conservation légale lorsque vous ne savez pas pendant combien de temps vous souhaitez que vos objets restent immuables. Cela peut être utile si un audit de externe vos données approche et que vous souhaitez que les objets restent immuables jusqu'à la fin de l'audit. Cela peut également servir si vous travaillez sur un projet qui utilise un jeu de données qui doit rester immuable jusqu'à la fin du projet.

Autorisations requises

Les opérations de verrouillage des objets nécessitent des autorisations spécifiques. En fonction de l'opération exacte que vous tentez de réaliser, vous aurez peut-être besoin de l'une des autorisations suivantes :

- `s3:BypassGovernanceRetention`
- `s3:GetBucketObjectLockConfiguration`
- `s3:GetObjectLegalHold`
- `s3:GetObjectRetention`

- `s3:PutBucketObjectLockConfiguration`
- `s3:PutObjectLegalHold`
- `s3:PutObjectRetention`

Pour obtenir la liste complète des autorisations Amazon S3 avec leurs descriptions, consultez Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service.

Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.

Pour en savoir plus sur l'utilisation de conditions avec les autorisations, consultez Exemples de politiques de compartiment utilisant des clés de condition.

Considérations relatives au verrouillage d'objet

Le verrouillage d'objet Amazon S3 permet d'empêcher la suppression ou le remplacement d'objets sur une période déterminée ou indéfinie.

Vous pouvez utiliser la console Amazon S3, AWS Command Line Interface (AWS CLI) ou l'API REST Amazon S3 pour afficher ou définir les informations de verrouillage des objets. AWS SDKs Pour obtenir des informations générales sur les fonctionnalités de verrouillage d'objet S3, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

> **Important**
>
> - Après avoir activé le verrouillage d'objet sur un compartiment, vous ne pouvez pas désactiver le verrouillage d'objet ni interrompre la gestion des versions pour ce compartiment.
> - Les compartiments S3 avec verrouillage d'objet ne peuvent pas être utilisés comme compartiments de destination pour les journaux d'accès au serveur. Pour plus d'informations, consultez the section called "Enregistrement de l'accès au serveur".

Rubriques

- Autorisations d'affichage des informations de verrouillage
- Ignorer le mode de gouvernance

- Utilisation du verrouillage d'objet avec la réplication S3
- Utilisation du verrouillage d'objet avec un chiffrement
- Utilisation du verrouillage d'objet avec l'inventaire Amazon S3
- Gestion des politiques de cycle de vie S3 avec le verrouillage d'objet
- Gestion des marqueurs de suppression avec le verrouillage d'objet
- Utilisation de S3 Storage Lens avec le verrouillage d'objet
- Chargement d'objets dans un compartiment avec le verrouillage d'objet activé
- Configuration d'événements et de notifications
- Définition de limites sur les périodes de rétention à l'aide d'une politique de compartiment

Autorisations d'affichage des informations de verrouillage

Vous pouvez afficher par programmation le statut de verrouillage d'objet d'une version d'objet Amazon S3 à l'aide des opérations HeadObject ou GetObject. Les deux opérations renvoient le mode de rétention, Rétention jusqu'à la date, et le statut de conservation légale pour la version d'objet spécifiée. En outre, vous pouvez consulter le statut du verrouillage d'objet pour plusieurs objets de votre compartiment S3 à l'aide de l'inventaire S3.

Pour afficher le mode de conservation et la période de conservation d'une version d'objet, vous devez avoir l'autorisation `s3:GetObjectRetention`. Pour afficher le statut de conservation légale d'une version d'objet, vous devez avoir l'autorisation `s3:GetObjectLegalHold`. Pour afficher la configuration de rétention par défaut d'un compartiment, vous devez disposer de l'autorisation `s3:GetBucketObjectLockConfiguration`. Si vous effectuez une demande pour une configuration de verrouillage d'objet sur un compartiment pour lequel le verrouillage d'objet S3 n'est pas activé, Amazon S3 renvoie une erreur.

Ignorer le mode de gouvernance

Si vous disposez de l'autorisation `s3:BypassGovernanceRetention`, vous pouvez effectuer des opérations sur les versions d'objet verrouillées en mode de gouvernance comme si elles n'étaient pas protégées. Ces opérations incluent la suppression d'une version d'objet, le raccourcissement de la période de rétention ou la suppression de la période de rétention de verrouillage d'objet en plaçant une nouvelle demande `PutObjectRetention` avec des paramètres vides.

Afin d'ignorer le mode de gouvernance, vous devez indiquer explicitement dans votre demande que vous voulez l'ignorer. Pour ce faire, incluez l'`x-amz-bypass-governance-retention:trueen-`

tête dans votre demande d'opération d'`PutObjectRetention`API ou utilisez le paramètre équivalent avec les demandes effectuées via le AWS CLI ou AWS SDKs. La console S3 applique automatiquement cet en-tête pour les demandes effectuées via la console S3 si vous disposez de l'autorisation `s3:BypassGovernanceRetention`.

> **Note**
>
> L'ignorance du mode de gouvernance n'affecte pas le statut de conservation légale d'une version d'objet. Si une conservation légale est activée pour une version d'objet, cette conservation légale reste en vigueur et empêche que les demandes remplacent ou suppriment la version d'objet.

Utilisation du verrouillage d'objet avec la réplication S3

Vous pouvez utiliser le verrouillage d'objet avec la réplication S3 pour activer la copie automatique et asynchrone d'objets verrouillés et de leurs métadonnées de rétention entre des compartiments S3. Cela signifie que pour les objets répliqués, Amazon S3 utilise la configuration de verrouillage d'objet du compartiment source. En d'autres termes, si le verrouillage d'objet est activé sur le compartiment source, il doit également être activé sur les compartiments de destination. Si vous chargez un objet directement dans le compartiment de destination (en dehors de la réplication S3), il hérite du verrouillage d'objet du compartiment de destination. Lorsque vous utilisez la réplication, les objets d'un compartiment source sont répliqués vers un ou plusieurs compartiments de destination.

Pour configurer la réplication sur un compartiment avec Object Lock activé, vous pouvez utiliser la console S3 AWS CLI, l'API REST Amazon S3 ou AWS SDKs.

> **Note**
>
> Pour utiliser Object Lock avec la réplication, vous devez accorder deux autorisations supplémentaires sur le compartiment S3 source dans le rôle AWS Identity and Access Management (IAM) que vous utilisez pour configurer la réplication. Les deux autorisations supplémentaires sont `s3:GetObjectRetention` et `s3:GetObjectLegalHold`. Si le rôle dispose d'une déclaration d'autorisation `s3:Get*`, cette déclaration répond à l'exigence. Pour plus d'informations, consultez Configuration des autorisations pour la réplication en direct.
>
> Pour obtenir des informations générales sur la réplication S3, consultez Réplication d'objets au sein des régions et entre elles.

Pour examiner des exemples de configuration de la réplication S3, consultez Exemples de configuration de la réplication en direct.

Utilisation du verrouillage d'objet avec un chiffrement

Amazon S3 chiffre par défaut tous les nouveaux objets. Vous pouvez utiliser le verrouillage d'objet avec vos objets chiffrés. Pour de plus amples informations, veuillez consulter Protection des données à l'aide du chiffrement.

Le verrouillage d'objet contribue à empêcher la suppression et le remplacement d'objets Amazon S3, mais il ne protège pas contre la perte d'accès aux clés de chiffrement ni contre leur suppression. Par exemple, si vous chiffrez vos objets à l'aide d'un chiffrement AWS KMS côté serveur et que votre AWS KMS clé est supprimée, vos objets risquent de devenir illisibles.

Utilisation du verrouillage d'objet avec l'inventaire Amazon S3

Vous pouvez configurer l'inventaire Amazon S3 pour créer des listes d'objets dans un compartiment S3 selon une planification définie. Vous pouvez configurer l'inventaire Amazon S3 pour inclure les métadonnées de verrouillage d'objet suivantes pour vos objets :

- Date limite de rétention
- Mode de rétention
- Statut de conservation légale

Pour de plus amples informations, veuillez consulter Catalogage et analyse de vos données avec l'inventaire S3.

Gestion des politiques de cycle de vie S3 avec le verrouillage d'objet

Les configurations de gestion du cycle de vie des objets continuent à fonctionner normalement sur les objets protégés, y compris le placement des marqueurs de suppression. Toutefois, une version verrouillée d'un objet ne peut pas être supprimée par une politique d'expiration du cycle de vie S3. Le verrouillage d'objet est maintenu quelle que soit la classe de stockage dans laquelle réside l'objet et tout au long des transitions du cycle de vie S3 entre les classes de stockage.

Pour plus d'informations sur la gestion des cycles de vie d'objet, consultez Gestion du cycle de vie des objets.

Gestion des marqueurs de suppression avec le verrouillage d'objet

Même si vous ne pouvez pas supprimer une version d'objet protégée, vous pouvez continuer à créer un marqueur de suppression pour cet objet. Le placement d'un marqueur de suppression sur un objet n'a pas pour effet de supprimer l'objet ou des versions de celui-ci. Cependant, il conduit Amazon S3 à se comporter la plupart du temps comme si l'objet avait été supprimé. Pour plus d'informations, consultez Utilisation des marqueurs de suppression.

> **Note**
>
> Les marqueurs de suppression ne sont pas protégés par WORM, quelles que soient la période de rétention ou la conservation légale en place sur l'objet sous-jacent.

Utilisation de S3 Storage Lens avec le verrouillage d'objet

Pour consulter les statistiques relatives aux nombres d'objets et d'octets de stockage avec verrouillage d'objets activé, vous pouvez utiliser Amazon S3 Storage Lens. S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets.

Pour plus d'informations, consultez Utilisation de S3 Storage Lens pour protéger vos données.

Pour obtenir une liste complète des métriques, consultez Glossaire des métriques Amazon S3 Storage Lens.

Chargement d'objets dans un compartiment avec le verrouillage d'objet activé

L'en-tête `Content-MD5` ou `x-amz-sdk-checksum-algorithm` est requis pour toute demande de chargement d'un objet dont la période de conservation est configurée à l'aide du verrouillage d'objet. Ces en-têtes permettent de vérifier l'intégrité de votre objet lors du chargement.

Lorsque vous chargez un objet à l'aide de la console Amazon S3, S3 ajoute automatiquement l'en-tête `Content-MD5`. Vous pouvez éventuellement spécifier une fonction de somme de contrôle supplémentaire et une valeur de somme de contrôle via la console en tant qu'en-tête `x-amz-sdk-checksum-algorithm`. Si vous utilisez l'PutObjectAPI, vous devez spécifier l'`Content-MD5`en-tête, l'`x-amz-sdk-checksum-algorithm`en-tête ou les deux pour configurer la période de rétention d'Object Lock.

Pour de plus amples informations, veuillez consulter Vérification de l'intégrité des objets dans Amazon S3.

Configuration d'événements et de notifications

Vous pouvez utiliser les notifications d'événements Amazon S3 pour suivre l'accès et les modifications apportées à vos configurations et données Object Lock en utilisant AWS CloudTrail. Pour plus d'informations CloudTrail, voir Qu'est-ce que c'est AWS CloudTrail ? dans le guide de AWS CloudTrail l'utilisateur.

Vous pouvez également utiliser Amazon CloudWatch pour générer des alertes sur la base de ces données. Pour plus d'informations CloudWatch, consultez le document Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon.

Définition de limites sur les périodes de rétention à l'aide d'une politique de compartiment

Vous pouvez définir des périodes de rétention autorisées minimale et maximale pour un compartiment en utilisant une politique de compartiment. La période de conservation maximale est de 100 ans.

L'exemple suivant montre une politique de compartiment qui utilise la clé de condition `s3:object-lock-remaining-retention-days` pour définir une période de conservation maximale de 10 jours.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "SetRetentionLimits",
    "Statement": [
        {
            "Sid": "SetRetentionPeriod",
            "Effect": "Deny",
            "Principal": "*",
            "Action": [
                "s3:PutObjectRetention"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
            "Condition": {
                "NumericGreaterThan": {
```

```
                    "s3:object-lock-remaining-retention-days": "10"
                }
            }
        }
    ]
}
```

> **Note**
>
> Si votre compartiment est le compartiment de destination d'une configuration de réplication, vous pouvez configurer des périodes de rétention minimale et maximale autorisées pour les réplicas d'objet créés à l'aide de la réplication. Pour ce faire, vous devez autoriser l'action `s3:ReplicateObject` dans votre politique de compartiment. Pour plus d'informations sur les autorisations de réplication, consultez the section called "Configurer les autorisations".

Pour plus d'informations sur les politiques de compartiment, consultez les rubriques suivantes :

- Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service

  Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.
- Opérations d'objet
- Exemples de politiques de compartiment utilisant des clés de condition

Configuration du verrouillage d'objet S3

Avec Amazon S3 Object Lock, vous pouvez stocker des objets dans des compartiments à usage général Amazon S3 à l'aide d'un modèle write-once-read-many(WORM). En utilisant le verrouillage des objets S3, vous pouvez empêcher qu'un objet ne soit supprimé ou remplacé sur une période déterminée ou indéfinie. Pour obtenir des informations générales sur les fonctionnalités du verrouillage d'objet, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

Avant de verrouiller des objets, vous devez activer le versionnage S3 et le verrouillage des objets sur un compartiment à usage général. Vous pouvez ensuite définir une période de rétention, une conservation légale ou les deux.

Pour utiliser le verrouillage d'objet, vous devez disposer de certaines autorisations. Pour obtenir la liste des autorisations associées aux différentes opérations de verrouillage d'objet, consultez the section called "Autorisations requises".

> **Important**
>
> - Après avoir activé le verrouillage d'objet sur un compartiment, vous ne pouvez pas désactiver le verrouillage d'objet ni interrompre la gestion des versions pour ce compartiment.
> - Les compartiments S3 avec verrouillage d'objet ne peuvent pas être utilisés comme compartiments de destination pour les journaux d'accès au serveur. Pour de plus amples informations, veuillez consulter the section called "Enregistrement de l'accès au serveur".

Rubriques

- Activer le verrouillage des objets lors de la création d'un nouveau compartiment S3 à usage général
- Activation du verrouillage d'objet sur un compartiment S3 existant
- Définition ou modification d'une conservation légale sur un objet S3
- Définition ou modification d'une période de rétention sur un objet S3
- Définition ou modification d'une période de rétention par défaut sur un compartiment S3

Activer le verrouillage des objets lors de la création d'un nouveau compartiment S3 à usage général

Vous pouvez activer Object Lock lors de la création d'un nouveau compartiment S3 à usage général à l'aide de la console Amazon S3 AWS SDKs, AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Choisissez Créer un compartiment.

La page Créer un compartiment s'ouvre.

4. Pour Nom du compartiment, saisissez le nom de votre compartiment.

> **Note**
>
> Après avoir créé un compartiment, vous ne pouvez pas modifier son nom. Pour plus d'informations sur l'attribution de noms à des compartiments, consultez Règles de dénomination des compartiments à usage général.

5. Pour Région, choisissez l' Région AWS endroit où vous souhaitez que le compartiment réside.
6. Sous Propriété des objets, choisissez de désactiver ou d'activer les listes de contrôle d'accès (ACLs) et de contrôler la propriété des objets chargés dans votre bucket.
7. Dans Paramètres de blocage de l'accès public pour ce compartiment, choisissez les paramètres Bloquer l'accès public que vous souhaitez appliquer au compartiment.
8. Sous Gestion des versions de compartiment, choisissez Activée.

   Le verrouillage d'objet fonctionne uniquement avec des compartiments versionnés.
9. (Facultatif) Sous Tags (Balises), vous pouvez choisir d'ajouter des balises à votre compartiment. Les balises sont des paires clé-valeur utilisées pour classer le stockage et allouer des coûts.
10. Sous Paramètres avancés, recherchez Verrouillage d'objet et choisissez Activer.

    Vous devez reconnaître que l'activation du verrouillage d'objet permettra de verrouiller définitivement les objets de ce compartiment.
11. Choisissez Créer un compartiment.

À l'aide du AWS CLI

L'exemple `create-bucket` suivant crée un nouveau compartiment S3 nommé *`amzn-s3-demo-bucket1`* avec le verrouillage d'objet activé :

```
aws s3api create-bucket --bucket amzn-s3-demo-bucket1 --object-lock-enabled-for-bucket
```

Pour plus d'informations et des exemples, voir create-bucketdans la référence de AWS CLI commande.

> **Note**
>
> Vous pouvez exécuter AWS CLI des commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? dans le guide de AWS CloudShell l'utilisateur.

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour créer un nouveau compartiment S3 avec le verrouillage d'objet activé. Pour plus d'informations, consultez .CreateBucketdans le manuel Amazon Simple Storage Service API Reference.

À l'aide du AWS SDKs

Pour savoir comment activer le verrouillage des objets lors de la création d'un nouveau compartiment S3 avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour des exemples expliquant comment obtenir la configuration actuelle de Object Lock avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour un scénario interactif illustrant différentes fonctionnalités de verrouillage d'objets à l'aide de AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Activation du verrouillage d'objet sur un compartiment S3 existant

Vous pouvez activer Object Lock pour un compartiment S3 existant à l'aide de la console Amazon S3, de l' AWS CLI API REST Amazon S3 ou de l'API REST Amazon S3. AWS SDKs

Utilisation de la console S3

> **Note**
>
> Le verrouillage d'objet fonctionne uniquement avec des compartiments versionnés.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment sur lequel vous souhaitez activer le verrouillage d'objet.
4. Choisissez l'onglet Propriétés.
5. Sous Propriétés, faites défiler l'affichage jusqu'à la section Verrouillage d'objet et choisissez Modifier.
6. Sous Verrouillage d'objet, choisissez Activer.

   Vous devez reconnaître que l'activation du verrouillage d'objet permettra de verrouiller définitivement les objets de ce compartiment.
7. Sélectionnez Enregistrer les modifications.

À l'aide du AWS CLI

L'exemple de commande `put-object-lock-configuration` suivant définit une période de rétention de verrouillage d'objet de 50 jours sur un compartiment nommé *`amzn-s3-demo-bucket1`* :

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

Pour plus d'informations et des exemples, voir put-object-lock-configurationdans la référence de AWS CLI commande.

> **Note**
>
> Vous pouvez exécuter AWS CLI des commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? dans le guide de AWS CloudShell l'utilisateur.

Utilisation de l'API REST

Vous pouvez utiliser l'API REST Amazon S3 pour activer le verrouillage d'objet sur un compartiment S3 existant. Pour plus d'informations, consultez .PutObjectLockConfigurationdans le manuel Amazon Simple Storage Service API Reference.

À l'aide du AWS SDKs

Pour savoir comment activer le verrouillage d'objets pour un compartiment S3 existant avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour des exemples expliquant comment obtenir la configuration actuelle de Object Lock avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour un scénario interactif illustrant différentes fonctionnalités de verrouillage d'objets à l'aide de AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Définition ou modification d'une conservation légale sur un objet S3

Vous pouvez définir ou supprimer un blocage légal sur un objet S3 à l'aide de la console Amazon S3 ou de l'API REST Amazon S3. AWS CLI AWS SDKs

> **Important**
>
> - Si vous souhaitez définir une conservation légale sur un objet, le verrouillage d'objet doit déjà être activé sur le compartiment de l'objet.
> - Lorsque vous placez (PUT) une version d'objet dotée d'un mode et d'une période de rétention individuels explicites dans un compartiment, les paramètres individuels de verrouillage d'objet de la version de l'objet remplacent tous les paramètres de rétention des propriétés du compartiment.

Pour plus d'informations, consultez the section called "Conservations légales".

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment qui contient l'objet sur lequel vous souhaitez définir ou modifier une conservation légale.
4. Dans la liste Objets, sélectionnez l'objet sur lequel vous souhaitez définir ou modifier une conservation légale.
5. Sur la page Propriétés de l'objet, recherchez la section Conservation légale du verrouillage d'objet et choisissez Modifier.
6. Choisissez Activer pour définir une conservation légale ou Désactiver pour supprimer une conservation légale.
7. Sélectionnez Enregistrer les modifications.

À l'aide du AWS CLI

L'exemple `put-object-legal-hold` suivant définit une conservation légale sur l'objet *`my-image.fs`* dans le compartiment nommé *`amzn-s3-demo-bucket1`* :

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=ON"
```

L'exemple `put-object-legal-hold` suivant supprime une conservation légale sur l'objet *`my-image.fs`* dans le compartiment nommé *`amzn-s3-demo-bucket1`* :

```
aws s3api put-object-legal-hold --bucket amzn-s3-demo-bucket1 --key my-image.fs --
legal-hold="Status=OFF"
```

Pour plus d'informations et des exemples, voir put-object-legal-holddans la référence de AWS CLI commande.

> **Note**
>
> Vous pouvez exécuter AWS CLI des commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous

pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? dans le guide de AWS CloudShell l'utilisateur.

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour définir ou modifier une conservation légale sur un objet. Pour plus d'informations, consultez .PutObjectLegalHolddans le manuel Amazon Simple Storage Service API Reference.

À l'aide du AWS SDKs

Pour des exemples sur la manière de définir une conservation légale sur un objet avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour savoir comment obtenir le statut de blocage légal actuel avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour un scénario interactif illustrant différentes fonctionnalités de verrouillage d'objets à l'aide de AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Définition ou modification d'une période de rétention sur un objet S3

Vous pouvez définir ou modifier une période de rétention sur un objet S3 à l'aide de la console Amazon S3 ou de l'API REST Amazon S3. AWS CLI AWS SDKs

⚠ Important

- Si vous souhaitez définir une période de rétention sur un objet, le verrouillage d'objet doit déjà être activé sur le compartiment de l'objet.
- Lorsque vous placez (PUT) une version d'objet dotée d'un mode et d'une période de rétention individuels explicites dans un compartiment, les paramètres individuels de verrouillage d'objet de la version de l'objet remplacent tous les paramètres de rétention des propriétés du compartiment.

- Le seul moyen de supprimer un objet en mode de conformité avant l'expiration de sa date de conservation est de supprimer l'objet associé Compte AWS.

Pour de plus amples informations, veuillez consulter Périodes de rétention.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment qui contient l'objet sur lequel vous souhaitez définir ou modifier une période de rétention.
4. Dans la liste Objets, sélectionnez l'objet sur lequel vous souhaitez définir ou modifier une période de rétention.
5. Sur la page Propriétés de l'objet, recherchez la section Rétention Verrouillage d'objet et choisissez Modifier.
6. Sous Rétention, choisissez Activer pour définir une période de rétention ou Désactiver pour supprimer une période de rétention.
7. Si vous avez choisi Activer, sous Mode de rétention, choisissez Mode de gouvernance ou Mode de conformité. Pour plus d'informations, consultez Modes de conservation.
8. Sous Rétention jusqu'à la date, choisissez la date à laquelle vous souhaitez que la période de rétention se termine. Durant cette période, l'objet est protégé selon le modèle WORM et ne peut être ni remplacé ni supprimé. Pour plus d'informations, consultez Périodes de rétention.
9. Sélectionnez Save Changes (Enregistrer les modifications).

À l'aide du AWS CLI

L'exemple `put-object-retention` suivant définit une période de rétention sur l'objet *my-image.fs* dans le compartiment nommé *amzn-s3-demo-bucket1* jusqu'au 1er janvier 2025 :

```
aws s3api put-object-retention --bucket amzn-s3-demo-bucket1 --key my-image.fs --
retention='{ "Mode": "GOVERNANCE", "RetainUntilDate": "2025-01-01T00:00:00" }'
```

Pour plus d'informations et des exemples, voir put-object-retentiondans la référence de AWS CLI commande.

> **Note**
>
> Vous pouvez exécuter AWS CLI des commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? dans le guide de AWS CloudShell l'utilisateur.

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour définir une période de rétention sur un objet. Pour plus d'informations, consultez .PutObjectRetentiondans le manuel Amazon Simple Storage Service API Reference.

À l'aide du AWS SDKs

Pour des exemples de définition d'une période de rétention pour un objet avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour savoir comment obtenir la période de rétention d'un objet avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour un scénario interactif illustrant différentes fonctionnalités de verrouillage d'objets à l'aide de AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Définition ou modification d'une période de rétention par défaut sur un compartiment S3

Vous pouvez définir ou modifier une période de rétention par défaut sur un compartiment S3 à l'aide de la console Amazon S3 ou de l'API REST Amazon S3. AWS CLI AWS SDKs Vous spécifiez une durée, en jours ou en années, pendant laquelle chaque version d'objet placée dans le compartiment sera protégée.

Important

- Si vous souhaitez définir une période de rétention par défaut sur un compartiment, le verrouillage d'objet doit déjà être activé sur ce compartiment.
- Lorsque vous placez (PUT) une version d'objet dotée d'un mode et d'une période de rétention individuels explicites dans un compartiment, les paramètres individuels de verrouillage d'objet de la version de l'objet remplacent tous les paramètres de rétention des propriétés du compartiment.
- Le seul moyen de supprimer un objet en mode de conformité avant l'expiration de sa date de conservation est de supprimer l'objet associé Compte AWS.

Pour de plus amples informations, veuillez consulter Périodes de rétention.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment sur lequel vous souhaitez définir ou modifier une période de rétention par défaut.
4. Choisissez l'onglet Propriétés.
5. Sous Propriétés, faites défiler l'affichage jusqu'à la section Verrouillage d'objet et choisissez Modifier.
6. Sous Rétention par défaut, choisissez Activer pour définir une rétention par défaut ou Désactiver pour supprimer une rétention par défaut.
7. Si vous avez choisi Activer, sous Mode de rétention, choisissez Mode de gouvernance ou Mode de conformité. Pour plus d'informations, consultez Modes de conservation.
8. Sous Période de rétention par défaut, choisissez le nombre de jours ou d'années que vous souhaitez comme période de rétention. Les objets placés dans ce compartiment seront verrouillés pendant ce nombre de jours ou d'années. Pour plus d'informations, consultez Périodes de rétention.
9. Sélectionnez Save Changes (Enregistrer les modifications).

À l'aide du AWS CLI

L'exemple de commande `put-object-lock-configuration` suivant définit une période de rétention de verrouillage d'objet de 50 jours sur le compartiment nommé *amzn-s3-demo-bucket1* en utilisant le mode de conformité :

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-
lock-configuration='{ "ObjectLockEnabled": "Enabled", "Rule": { "DefaultRetention":
 { "Mode": "COMPLIANCE", "Days": 50 }}}'
```

L'exemple `put-object-lock-configuration` suivant supprime la configuration de rétention par défaut sur un compartiment :

```
aws s3api put-object-lock-configuration --bucket amzn-s3-demo-bucket1 --object-lock-
configuration='{ "ObjectLockEnabled": "Enabled"}'
```

Pour plus d'informations et des exemples, voir put-object-lock-configurationdans la référence de AWS CLI commande.

> **Note**
>
> Vous pouvez exécuter AWS CLI des commandes depuis la console en utilisant AWS CloudShell. AWS CloudShell est un shell pré-authentifié basé sur un navigateur que vous pouvez lancer directement depuis le. AWS Management Console Pour plus d'informations, voir Qu'est-ce que c'est CloudShell ? dans le guide de AWS CloudShell l'utilisateur.

Utilisation de l'API REST

Vous pouvez utiliser l'API REST pour définir une période de conservation par défaut sur un compartiment S3 existant. Pour plus d'informations, consultez .PutObjectLockConfigurationdans le manuel Amazon Simple Storage Service API Reference.

À l'aide du AWS SDKs

Pour des exemples de définition d'une période de rétention par défaut sur un compartiment S3 existant avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour un scénario interactif illustrant différentes fonctionnalités de verrouillage d'objets à l'aide de AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Pour obtenir des informations générales sur l'utilisation de différents AWS SDKs éléments, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence sur les API Amazon S3.

Sauvegarde de vos données Amazon S3

Amazon S3 est intégré de manière native à AWS Backup un service entièrement géré basé sur des politiques que vous pouvez utiliser pour définir de manière centralisée des politiques de sauvegarde afin de protéger vos données dans Amazon S3. Une fois que vous avez défini vos politiques de sauvegarde et attribué des ressources Amazon S3 à ces politiques, vous avez AWS Backup automatisé la création de sauvegardes Amazon S3 et les avez stockées en toute sécurité dans un coffre-fort de sauvegarde crypté que vous avez désigné dans votre plan de sauvegarde.

Lorsque vous utilisez AWS Backup Amazon S3, vous pouvez effectuer les actions suivantes :

- Créez des sauvegardes continues et des sauvegardes périodiques. Les sauvegardes continues sont utiles pour la point-in-time restauration, et les sauvegardes périodiques sont utiles pour répondre à vos besoins de conservation des données à long terme.
- Automatisez la planification et la rétention des sauvegardes en configurant les stratégies de sauvegarde de manière centralisée.
- Restaurez les sauvegardes des données Amazon S3 à un point dans le temps que vous spécifiez.

Vous pouvez également utiliser le versionnement S3 et la réplication S3 pour vous aider à récupérer après des suppressions accidentelles et à effectuer vos propres opérations de restauration automatique. AWS Backup

Prérequis

Vous devez activer la gestion des versions S3 sur votre compartiment avant de AWS Backup pouvoir le sauvegarder.

> **Note**
>
> Nous vous recommandons de définir une règle d'expiration du cycle de vie pour les compartiments compatibles avec la gestion des versions qui sont sauvegardés. Si vous ne

définissez pas de période d'expiration du cycle de vie, vos coûts de stockage Amazon S3 risquent d'augmenter car AWS Backup conserve toutes les versions de vos données Amazon S3.

Premiers pas

AWS Backup Pour commencer à utiliser Amazon S3, consultez la section Création de sauvegardes Amazon S3 dans le guide du AWS Backup développeur.

Restrictions et limitations

Pour en savoir plus sur les limites, consultez Création des sauvegardes Amazon S3 dans le Guide du développeur AWS Backup .

Optimisation des coûts

Amazon S3 offre une gamme de fonctionnalités et de classes de stockage pour vous aider à optimiser les coûts tout au long du cycle de vie de vos données. Les classes de stockage offrent la flexibilité nécessaire pour gérer vos coûts, en fournissant différents niveaux d'accès aux données aux coûts correspondants, sans frais initiaux ni engagement quant à la quantité de contenu que vous stockez. Comme les autres AWS services, vous payez au fur et à mesure et vous ne payez que pour ce que vous utilisez.

Les classes de stockage Amazon S3 sont spécialement conçues pour fournir le stockage le moins coûteux pour différents modèles d'accès. Il s'agit des licences suivantes :

- S3 Standard pour le stockage à usage général de données fréquemment consultées.
- Amazon S3 Express One Zone pour des données hautes performances fréquemment consultées dans une zone de disponibilité unique.
- S3 Intelligent-Tiering pour optimiser automatiquement les coûts pour les données dont les modèles d'accès sont inconnus ou variables.
- S3 Standard-IA (S3 Standard-IA) et S3 One Zone-IA (S3 One Zone-IA) pour les données de longue durée, mais moins fréquemment consultées.
- S3 Glacier Instant Retrieval pour les données d'archive nécessitant un accès immédiat.
- S3 Glacier pour les données d'archive qui ne nécessitent pas un accès immédiat mais qui ont besoin de la flexibilité nécessaire pour récupérer gratuitement de grands jeux de données.
- S3 Glacier Deep Archive pour l'archivage à long terme et la préservation numérique aux coûts de stockage les plus bas dans le cloud.

Vous pouvez déplacer des objets vers la classe de stockage la plus économique à tout moment. En outre, Amazon S3 fournit des fonctionnalités pour gérer le cycle de vie de vos données. Par exemple, vous pouvez utiliser la configuration du cycle de vie S3 pour automatiser la transition des objets vers des classes de stockage plus économiques ou pour supprimer automatiquement les objets expirés en fonction de règles que vous définissez.

Des fonctionnalités telles que l'analyse des classes de stockage S3, le balisage de répartition des coûts et les rapports de facturation et d'utilisation vous aident à analyser vos modèles de coûts et d'utilisation.

Rubriques

- Rapports d'utilisation et de facturation pour Amazon S3
- Bien comprendre et gérer les classes de stockage Amazon S3
- Gestion du cycle de vie des objets

Rapports d'utilisation et de facturation pour Amazon S3

Lorsque vous utilisez Amazon S3, vous n'avez rien à payer d'avance et n'avez pas à vous engager sur le volume de votre stockage. Comme les autres Services AWS, vous payez au fur et à mesure et vous ne payez que pour ce que vous utilisez.

AWS fournit les rapports suivants pour Amazon S3 :

- Rapports de facturation : plusieurs rapports fournissant des vues détaillées de toutes les activités liées au produit Services AWS que vous utilisez, y compris Amazon S3. AWS facture toujours au propriétaire du compartiment S3 les frais Amazon S3, sauf si le compartiment a été créé en tant que compartiment Requester Pays. Pour en savoir plus sur les compartiments de ce type, consultez Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation. Pour en savoir plus sur les rapports de facturation, consultez AWS Billing rapports pour Amazon S3.
- Rapport d'utilisation – Résumé des activités pour un service spécifique, avec les totaux horaires, quotidiens ou mensuels. Vous voulez choisir le type d'utilisation et les opérations à inclure. Vous pouvez également choisir la manière dont les données sont regroupées. Pour plus d'informations, consultez AWS rapports d'utilisation pour Amazon S3.

Les rubriques suivantes fournissent des informations sur les rapports d'utilisation et de facturation pour Amazon S3.

Rubriques

- Utilisation des balises de répartition des coûts pour les compartiments S3
- AWS Billing rapports pour Amazon S3
- AWS rapports d'utilisation pour Amazon S3
- Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3
- Facturation des réponses d'erreur Amazon S3

Utilisation des balises de répartition des coûts pour les compartiments S3

Pour effectuer le suivi des coûts de stockage ou d'autres éléments pour des projets ou groupes de projets, étiquetez vos compartiments Amazon S3 à l'aide de balises de répartition des coûts. Une balise de répartition des coûts correspond à une paire clé-valeur que vous associez à un compartiment S3. Après avoir activé les balises de répartition des coûts, AWS utilise les balises pour organiser les coûts des ressources dans votre rapport de répartition des coûts. Les balises de répartition des coûts ne peuvent être utilisées que pour nommer les compartiments. Pour en savoir plus sur les balises utilisées pour la dénomination d'objets, consultez Catégorisation de vos objets à l'aide de balises.

Le rapport de répartition des coûts répertorie l' AWS utilisation de votre compte par catégorie de produit et par utilisateur du compte associé. Il contient les mêmes postes que le rapport de facturation détaillée (consultez Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3), ainsi que des colonnes supplémentaires pour vos clés de balises.

AWS fournit deux types de balises de répartition des coûts, une balise AWS générée et une balise définie par l'utilisateur. AWS définit, crée et applique la `createdBy` balise AWS générée pour vous après un CreateBucket événement Amazon S3. Vous pouvez définir, créer et appliquer des balises définies par l'utilisateur à votre compartiment S3.

Vous devez activer ces deux types de balises séparément dans la console de gestion des coûts et de la facturation pour qu'elles apparaissent dans vos rapports de facturation. Pour plus d'informations sur les balises AWS-générées, voir AWS-Generated Cost Allocation Tags.

Pour de plus amples informations sur l'activation de balises, veuillez consulter Utilisation des étiquettes de répartition des coûts dans le Guide de l'utilisateur AWS Billing .

Balises de répartition des coûts définies par l'utilisateur

Une balise de répartition des coûts définie par l'utilisateur comprend les composants suivants :

- Clé de balise . il s'agit du nom de la balise. Par exemple, dans la balise projet/Trinity, projet est la clé. La balise est sensible à la casse et doit contenir entre 1 et 128 caractères Unicode.

- Valeur de balise. Il s'agit d'une chaîne obligatoire. Par exemple, dans la balise projet/Trinity, Trinity est la valeur. La valeur de clé est sensible à la casse et doit contenir entre 0 et 256 caractères Unicode.

Pour connaître les caractères autorisés dans les étiquettes définies par l'utilisateur et les autres restrictions, veuillez consulter la section Restrictions encadrant les étiquettes définies par l'utilisateur du Guide de l'utilisateur AWS Billing . Pour de plus amples informations sur les étiquettes définies par l'utilisateur, veuillez consulter la section Étiquettes de répartition des coûts définies par l'utilisateur du Guide de l'utilisateur AWS Billing .

Balises de compartiment S3

Chaque compartiment S3 possède un ensemble de balises. Un ensemble de balises contient toutes les balises associées au compartiment. Un ensemble de balises peut contenir jusqu'à 50 balises ou n'en contenir aucune. Dans un ensemble de balises, les clés doivent être uniques, contrairement aux valeurs. Par exemple, vous pouvez avoir la même valeur dans les ensembles de balises nommés project/Trinity et Cost-Center/Trinity.

Si, dans un compartiment, vous ajoutez une balise qui dispose de la même clé qu'une balise existante, la nouvelle valeur remplace l'ancienne valeur.

AWS n'applique aucune signification sémantique à vos balises. Nous interprétons les balises de façon stricte, en tant que chaîne de caractères.

Pour ajouter, répertorier, modifier ou supprimer des balises, vous pouvez utiliser la console Amazon S3, le AWS Command Line Interface (AWS CLI) ou l'API Amazon S3.

Gestion des balises pour les compartiments à usage général

Vous pouvez ajouter ou gérer des balises pour des compartiments à usage général à l'aide de la console Amazon S3, de l'interface de ligne de AWS commande (CLI) AWS SDKs, du ou à l'aide du S3 APIs. Pour plus d'informations, consultez les rubriques suivantes.

Utilisation de la console Amazon S3

Pour créer des balises dans la console, voir :

- Afficher les propriétés d'un bucket S3 à usage général.

Utilisation de l'API

Pour gérer les balises à l'aide de l'API Amazon S3, consultez les pages d'API suivantes dans le manuel Amazon Simple Storage Service API Reference.

- PutBucketTagging
- GetBucketTagging
- DeleteBucketTagging

Utilisation de l' CLI

Pour gérer les balises à l'aide de AWS CLI, consultez les pages suivantes dans le manuel de référence des AWS CLI commandes.

- put-bucket-tagging
- get-bucket-tagging
- delete-bucket-tagging

Plus d'informations

- Utilisation des étiquettes de répartition des coûts dans le Guide de l'utilisateur AWS Billing .
- Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3
- AWS Billing rapports pour Amazon S3

AWS Billing rapports pour Amazon S3

Votre facture mensuelle AWS sépare vos informations d'utilisation et vos coûts par Service AWS fonction. Plusieurs AWS Billing rapports sont disponibles : le rapport mensuel, le rapport de répartition des coûts et les rapports de facturation détaillés. Pour plus d'informations sur l'affichage de vos rapports de facturation, consultez Affichage d'une facture dans le Guide de l'utilisateur AWS Billing .

Pour suivre votre AWS utilisation et fournir une estimation des frais associés à votre compte, vous pouvez configurer AWS Cost and Usage Reports. Pour plus d'informations, voir Qu'est-ce que c'est AWSCost and Usage Reports ? dans le Guide d'exportation de AWS données.

Vous pouvez également télécharger un rapport d'utilisation, qui fournit plus d'informations sur votre utilisation du stockage Amazon S3 que les rapports de facturation. Pour plus d'informations, consultez AWS rapports d'utilisation pour Amazon S3.

Le tableau suivant répertorie les coûts liés à l'utilisation d'Amazon S3.

Opération payante	Commentaires
Stockage	Des frais de stockage d'objets dans vos compartiments S3 vous sont facturés. Le tarif qui vous est facturé dépend de la taille de vos objets, de leur durée de stockage au cours du mois et de leur classe de stockage. Amazon S3 propose les classes de stockage suivantes : S3 Standard, S3 Express One Zone, S3 Intelligent-Tiering, S3 Standard-IA (IA signifie Accès peu fréquent), S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval, S3 Glacier Deep Archive ou Reduced Redundancy Storage (RRS). Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3. Sachez que si la gestion des versions S3 est activée, vous êtes facturé pour chaque version d'un objet conservé. Pour plus d'informations sur la gestion des versions, consultez Fonctionnement de la gestion des versions S3.
Compartiments à usage général	Les 2 000 premiers compartiments à usage général que vous créez dans votre compte ne vous sont pas facturés. Toutefois, il existe un tarif par compartiment pour chaque compartiment que vous créez au-delà des 2 000 premiers. Ce tarif est facturé par compartiment/mois. Pour obtenir des informations sur la tarification des compartiments à usage général, consultez Tarification Amazon S3.
Surveillance et automatisation	Vous payez mensuellement des frais de surveillance et d'automatisation par objet stocké dans la classe de stockage S3 Intelligent-Tiering. Cela permet de surveiller les

Opération payante	Commentaires
	modèles d'accès et de déplacer les objets dans les niveaux d'accès au sein de la dite classe.
Requêtes	Vous payez pour les demandes, par exemple les demandes `GET`, émises sur vos objets et compartiments S3. Les demandes liées au cycle de vie sont incluses. Le montant facturé pour les demandes dépend du type des demandes émises. Pour plus d'informations sur la tarification des demandes, consultez Tarification Amazon S3.
Extractions	Des frais vous sont facturés pour l'extraction d'objets stockés dans les espaces de stockage S3 Standard-IA, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.
Suppressions anticipées	Si vous supprimez un objet stocké dans un espace de stockage S3 Standard-IA, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive avant expiration du délai de stockage minimum pour lequel vous vous êtes engagé, des frais de suppression anticipée vous sont facturés pour l'objet en question.
Gestion du stockage	Vous payez pour les fonctionnalités de gestion du stockage (inventaire Amazon S3, analytique et balisage des objets) activées sur les compartiments de votre compte.

Opération payante	Commentaires
Bande passante	Vous payez pour l'ensemble de la bande passante entrante et sortante dans Amazon S3, à l'exception des éléments ci-dessous : • Données transférées depuis Internet • Données transférées vers une instance Amazon Elastic Compute Cloud (Amazon EC2), lorsque l'instance se trouve dans le même compartiment Région AWS que le compartiment S3 • Données transférées vers Amazon CloudFront (CloudFront) Vous payez également des frais pour tout transfert de données via Amazon S3 Transfer Acceleration.

Pour des informations détaillées sur les frais d'utilisation d'Amazon S3 pour le stockage, le transfert de données et les services, consultez les tarifs Amazon S3 et Amazon S3 FAQs.

Pour obtenir des informations sur les codes et abréviations utilisés dans les rapports d'utilisation et de facturation pour Amazon S3, consultez Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3.

Plus d'informations

- AWS rapports d'utilisation pour Amazon S3
- Utilisation des balises de répartition des coûts pour les compartiments S3
- AWS Billing et gestion des coûts
- Tarification Amazon S3

AWS rapports d'utilisation pour Amazon S3

Lorsque vous téléchargez un rapport d'utilisation, vous pouvez demander à cumuler les données d'utilisation sur une base horaire, quotidienne ou mensuelle. Le rapport d'utilisation d'Amazon S3 répertorie les opérations par type d'utilisation et Région AWS. Pour des rapports plus détaillés sur l'utilisation de l'espace de stockage Amazon S3, téléchargez les rapports d'utilisation AWS générés de façon dynamique. Vous voulez choisir le type d'utilisation, les opérations et la période à inclure. Vous pouvez également choisir la manière dont les données sont regroupées. Pour plus d'informations sur les rapports d'utilisation, consultez Rapport d'utilisation AWS dans le Guide de l'utilisateur AWS Data Exports.

Le rapport d'utilisation Amazon S3 inclut les informations suivantes :

- Service – Amazon S3
- Operation – Opération effectuée sur votre compartiment ou objet. Pour obtenir une explication détaillée des opérations Amazon S3, consultez Opérations de suivi dans vos rapports d'utilisation.
- UsageType— L'une des valeurs suivantes :
  - Code qui identifie le type de stockage
  - Code qui identifie le type de demande
  - Code qui identifie le type d'extraction
  - Code qui identifie le type de transfert de données
  - Code qui identifie les suppressions anticipées dans les espaces de stockage S3 Intelligent-Tiering, S3 standard – Accès peu fréquent, S3 One Zone-Infrequent Access (S3 One Zone-IA), S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive
  - `StorageObjectCount` – Nombre d'objets stockés dans un compartiment donné

  Pour obtenir une explication détaillée des types d'utilisation d'Amazon S3, consultez Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3.
- Ressource : nom du compartiment ou de la table associé à l'utilisation répertoriée.
- StartTime— Heure de début de la journée à laquelle s'applique l'utilisation, en temps universel coordonné (UTC).
- EndTime— Heure de fin de la journée à laquelle s'applique l'utilisation, en temps universel coordonné (UTC).

- UsageValue— L'une des valeurs de volume suivantes. L'unité de mesure standard des données est le gigaoctet (Go). Toutefois, selon le service et le rapport, des téraoctets (To) peuvent apparaître à la place.
  - Nombre de requêtes au cours de la période spécifiée
  - Volume de données transférées
  - Volume de données stockées dans une heure donnée
  - Volume de données associées à des restaurations à partir d'un espace de stockage S3 Standard-IA, S3 One Zone-IA, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive

> **Tip**
>
> Pour plus d'informations sur les demandes reçues par Amazon S3 pour vos objets, activez la journalisation des accès serveur de vos compartiments. Pour plus d'informations, consultez Enregistrement de demandes avec journalisation des accès au serveur.

Vous pouvez télécharger un rapport d'utilisation au format XML ou CSV (séparé par des virgules). Voici un exemple de rapport d'utilisation au format CSV ouvert dans un tableur.

Service	Operation	UsageType	Resource	StartTime	EndTime	UsageValue
AmazonS3	HeadBucket	USW2-C3DataTransfer-Out-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	15309
AmazonS3	PutObject	USW2-C3DataTransfer-In-Bytes	admin-created3	6/1/2017 0:00	7/1/2017 0:00	19062
AmazonS3	HeadBucket	USW2-Requests-Tier2	admin-created3	6/1/2017 0:00	7/1/2017 0:00	68
AmazonS3	PutObjectForRepl	USW1-Requests-SIA-Tier1	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	178294
AmazonS3	PutObjectForRepl	USW1-USW2-AWS-In-Bytes	ca-example-bucket	6/1/2017 0:00	7/1/2017 0:00	387929083
AmazonS3	GetObjectForRepl	USW2-Requests-NoCharge	admin-created3	6/1/2017 0:00	7/1/2017 0:00	108
AmazonS3	GetObjectForRepl	USW2-USW1-AWS-Out-Bytes	my-test-bucket-bash	6/1/2017 0:00	7/1/2017 0:00	387910021

Pour de plus amples informations, veuillez consulter Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3.

Téléchargement du rapport AWS d'utilisation

Vous pouvez télécharger un rapport d'utilisation en tant que fichier XML ou CSV.

Pour télécharger le rapport d'utilisation

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans la barre de titre, choisissez votre nom d'utilisateur ou ID de compte, puis choisissez Facturation et gestion des coûts.
3. Dans le volet de navigation, choisissez Pages héritées et Rapports d'utilisation et de coûts.
4. Sous Rapport AWS d'utilisation, choisissez Créer un rapport d'utilisation.
5. Dans la page Télécharger le rapport d'utilisation, choisissez les paramètres suivants :
   - Services : choisissez Amazon Simple Storage Service.
   - Usage Types (Types d'utilisation) – Pour obtenir une explication détaillée des types d'utilisation Amazon S3, consultez Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3.
   - Operation (Opération) – Pour obtenir une explication détaillée des opérations Amazon S3, consultez Opérations de suivi dans vos rapports d'utilisation.
   - Period (Période) – Période que le rapport doit couvrir.
   - Report Granularity (Niveau de détail du rapport) – Indiquez si vous souhaitez que le rapport intègre les sous-totaux par heure, jour ou mois.
6. Choisissez Télécharger, choisissez le format de téléchargement (rapport XML ou rapport CSV), puis suivez les invites pour ouvrir ou enregistrer le rapport.

Plus d'informations

- Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3
- AWS Billing rapports pour Amazon S3

Comprendre vos rapports AWS de facturation et d'utilisation pour Amazon S3

Lorsque vous utilisez Amazon S3, nous incluons les codes associés dans vos rapports AWS de facturation et d'utilisation. L'examen de ces codes vous aide à comprendre les coûts et les habitudes d'utilisation d'Amazon S3. Le suivi et la gestion de vos dépenses sont essentiels pour optimiser vos coûts. Pour plus d'informations, consultez Tarification Amazon S3.

Les rapports d'utilisation et de facturation Amazon S3 utilisent des codes et abréviations. Pour les types d'utilisation figurant dans le tableau ci-dessous *`regionregion1`*, remplacez et par les abréviations *`region2`* des codes de Région AWS facturation du Guide de l'utilisateur des zones de disponibilitéRégions AWS et des zones de disponibilité.

Pour les types d'utilisation des points d'accès multi-régions S3 dans le tableau suivant, remplacez *regiongroup1* et *regiongroup2* par les abréviations figurant dans cette liste.

- AP : Asie-Pacifique
- AU : Australie
- EU : Europe
- IN : Inde
- NA : Amérique du Nord
- SA : Amérique du Sud

Les groupes de régions sont des regroupements géographiques de plusieurs Régions AWS. Pour plus d'informations, consultez Régions et zones de disponibilité. Pour obtenir des informations sur la tarification par Région AWS, consultez Tarification Amazon S3.

La première colonne du tableau suivant répertorie les types d'utilisation qui apparaissent dans les rapports d'utilisation et de facturation. L'unité de mesure standard des données est le gigaoctet (Go). Toutefois, selon le service et le rapport, des téraoctets (To) peuvent apparaître à la place.

Type d'utilisation	Unités	Granularité	Description
region1-*region2*-AWS-In-A Bytes	Go	Par heure	Quantité de données accélérées transférées vers *region1* depuis *region2*
region1-*region2*-AWS-In-A Bytes-T1	Go	Par heure	La quantité de données accélérées T1 transférées *region1* depuis*region2*, où T1 fait référence aux CloudFront demandes adressées à des points de présence (POPs) aux États-Unis d'Amérique, en Europe et au Japon

Type d'utilisation	Unités	Granularité	Description
region1-*region2*-AWS-In-A Bytes-T2	Go	Par heure	La quantité de données accélérées T2 transférées *region1* depuis*region2*, où T2 fait référence aux CloudFront demandes adressées POPs à tous les autres emplacements AWS périphériques
region1-*region2*-AWS-In-Bytes	Go	Par heure	Quantité de données transférées vers *region1* depuis *region2*
region1-*region2*-AWS-Out-ABytes	Go	Par heure	Quantité de données accélérées transférées de *region1* vers *region2*
region1-*region2*-AWS-Out-ABytes-T1	Go	Par heure	La quantité de données accélérées T1 transférées de *region1* à*region2*, T1 faisant référence aux CloudFront demandes adressées aux États-Unis d'Amérique, POPs en Europe et au Japon

Type d'utilisation	Unités	Granularité	Description
region1-*region2*-AWS-Out-ABytes-T2	Go	Par heure	La quantité de données accélérées T2 transférées de *region1* à*region2*, où T2 fait référence aux CloudFront demandes adressées POPs à tous les autres emplacements AWS périphériques
region1-*region2*-AWS-Out-Bytes	Go	Par heure	Quantité de données transférées de *region1* vers *region2*
region-BatchOperations-Jobs	Nombre	Par heure	Nombre de tâches S3 Batch Operations exécutées.
region-BatchOperations-Objects	Nombre	Par heure	Nombre d'opérations d'objets effectuées par S3 Batch Operations
region-Bulk-Retrieval-Bytes	Go	Par heure	Volume de données extraites à l'aide de demandes S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive en bloc
region-BytesDeleted-GDA	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject du stockage S3 Glacier Deep Archive

Type d'utilisation	Unités	Granularité	Description
region-BytesDeleted-GIR	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject du stockage S3 Glacier Instant Retrieval
region-BytesDeleted-GLACIER	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject du stockage S3 Glacier Flexible Retrieval
region-BytesDeleted-INT	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject du stockage S3 Intelligent-Tiering
region-BytesDeleted-RRS	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject à partir du stockage RRS (Reduced Redundancy Storage)
region-BytesDeleted-SIA	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject du stockage S3 Standard-IA
region-BytesDeleted-STANDARD	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject du stockage S3 Standard

Type d'utilisation	Unités	Granularité	Description
region-BytesDeleted-ZIA	Go	Mensuel	Quantité de données supprimées par une opération DeleteObject du stockage S3 One Zone-IA
region-C3DataTransfer-In-Bytes	Go	Par heure	La quantité de données transférée vers Amazon S3 depuis Amazon EC2 au sein du même Région AWS
region-C3DataTransfer-Out-Bytes	Go	Par heure	La quantité de données transférée d'Amazon S3 vers Amazon EC2 dans le même Région AWS
region-CloudFront-In-Bytes	Go	Par heure	La quantité de données transférées vers et Région AWS depuis une CloudFront distribution
region-CloudFront-Out-Bytes	Go	Par heure	La quantité de données transférée d'une CloudFront distribution Région AWS à une autre
region-DataTransfer-In-Bytes	Go	Par heure	Volume de données transférées vers Amazon S3 à partir d'internet
region-DataTransfer-Out-Bytes	Go	Par heure	Volume de données transférées depuis Amazon S3 vers internet[1]

Type d'utilisation	Unités	Granularité	Description
region-DataTransfer-Regional-Bytes	Go	Par heure	La quantité de données transférée depuis Amazon S3 vers les AWS ressources de ce dernier Région AWS
region-EarlyDelete-ByteHrs	Go-heures	Par heure	Volume d'utilisation du stockage, calculé au prorata, pour les objets supprimés de l'espace de stockage S3 Glacier Flexible Retrieval, avant expiration du délai d'engagement minimum de 90 jours[2]
region-EarlyDelete-GDA	Go-heures	Par heure	Volume d'utilisation du stockage, calculé au prorata, pour les objets supprimés de l'espace de stockage S3 Glacier Deep Archive, avant expiration du délai d'engagement minimum de 180 jours [2]
region-EarlyDelete-GIR	Go-heures	Par heure	Volume d'utilisation du stockage, calculé au prorata, pour les objets supprimés de l'espace de stockage S3 Glacier Instant Retrieval, avant expiration du délai d'engagement minimum de 90 jours

Type d'utilisation	Unités	Granularité	Description
region-EarlyDelete-GIR-SmObjects	Go-heures	Par heure	Volume d'utilisation du stockage, calculé au prorata, pour les petits objets (de moins de 128 Ko) qui ont été supprimés de S3 Glacier Instant Retrieval avant expiration du délai d'engagement minimum de 90 jours
region-EarlyDelete-SIA	Go-heures	Par heure	Volume d'utilisation du stockage, au prorata, pour les objets supprimés dans le stockage S3 standard – Accès peu fréquent, avant expiration du délai d'engagement minimum de 30 jours[3]
region-EarlyDelete-SIA-SmObjects	Go-heures	Par heure	Volume d'utilisation du stockage, au prorata, pour les petits objets (de moins de 128 Ko) qui ont été supprimés du stockage S3 standard – Accès peu fréquent avant expiration du délai d'engagement minimum de 30 jours[3]

Type d'utilisation	Unités	Granularité	Description
region-EarlyDelete-ZIA	Go-heures	Par heure	Volume d'utilisation du stockage, au prorata, pour les objets supprimés dans le stockage S3 One Zone-IA, avant expiration du délai d'engagement minimum de 30 jours[3]
region-EarlyDelete-ZIA-SmObjects	Go-heures	Par heure	Volume d'utilisation du stockage, au prorata, pour les petits objets (de moins de 128 Ko) qui ont été supprimés du stockage S3 One Zone-IA avant expiration du délai d'engagement minimum de 30 jours[3]
region-Expedited-Retrieval-Bytes	Go	Par heure	Volume de données extraites à l'aide de demandes S3 Glacier Flexible Retrieval accélérées
Global-Bucket-Hrs-FreeTier	Compartiment	Mensuel	Nombre de compartiments à usage général présents dans votre compte dans le cadre du niveau gratuit de 2 000 compartiments au niveau du compte

Type d'utilisation	Unités	Granularité	Description
`Global-Bucket-Hrs`	Compartiment	Mensuel	Nombre de compartiments à usage général présents dans votre compte au-delà du cadre du niveau gratuit de 2 000 compartiments au niveau du compte
region`-Inventory-Objects Listed`	Objets	Par heure	Nombre d'objets répertoriés pour un groupe d'objets (les objets sont regroupés par compartiment ou préfixe) avec une liste d'inventaire
region`-Metadata-Updates`	Mises à jour	Par heure	Frais par mise à jour pour les mises à jour traitées par les métadonnées S3
region`-Monitoring-Automation-INT`	Objets	Par heure	Nombre d'objets uniques surveillés et à niveau automatique de la classe de stockage S3 Intelligent-Tiering
region`-MRAP-Out-Bytes`	Go	Par heure	Quantité de données transférées via un point de terminaison de points d'accès multi-régions S3 hors des compartiments d'une région (tarification du routage des données MRAP).

Type d'utilisation	Unités	Granularité	Description
region-MRAP-In-Bytes	Go	Par heure	Quantité de données transférées via un point de terminaison de points d'accès multi-régions S3 hors des compartiments d'une région (tarification du routage des données MRAP).
regiongroup1-regiongroup2--MRAP-Out-Bytes	Go	Par heure	La quantité de données transférée via un point d'accès multirégional S3 depuis un compartiment *regiongroup1* vers un client *regiongroup2* situé en dehors du AWS réseau.
regiongroup1-regiongroup2--MRAP-In-Bytes	Go	Par heure	La quantité de données transférée via un point d'accès multirégional S3 vers un compartiment *regiongroup1* depuis un client *regiongroup2* situé en dehors du AWS réseau.
region-OverwriteBytes-Copy-GDA	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage S3 Glacier Deep Archive

Type d'utilisation	Unités	Granularité	Description
region-OverwriteBytes-Copy-GIR	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage S3 Glacier Instant Retrieval
region-OverwriteBytes-Copy-GLACIER	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage S3 Glacier Flexible Retrieval
region-OverwriteBytes-Copy-INT	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage S3 Intelligent-Tiering
region-OverwriteBytes-Copy-RRS	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage RRS (Reduced Redundancy Storage)
region-OverwriteBytes-Copy-SIA	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage S3 Standard-IA
region-OverwriteBytes-Copy-STANDARD	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage S3 Standard

Type d'utilisation	Unités	Granularité	Description
region-OverwriteBytes-Copy-ZIA	Go	Mensuel	Quantité de données écrasées par une opération CopyObject à partir du stockage S3 One Zone-IA
region-OverwriteBytes-Put-GDA	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage S3 Glacier Deep Archive
region-OverwriteBytes-Put-GIR	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage S3 Glacier Instant Retrieval
region-OverwriteBytes-Put-GLACIER	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage S3 Glacier Flexible Retrieval
region-OverwriteBytes-Put-INT	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage S3 Intelligent-Tiering
region-OverwriteBytes-Put-RRS	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage RRS (Reduced Redundancy Storage)

Type d'utilisation	Unités	Granularité	Description
region-OverwriteBytes-Put-SIA	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage S3 Standard-IA
region-OverwriteBytes-Put-STANDARD	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage S3 Standard
region-OverwriteBytes-Put-ZIA	Go	Mensuel	Quantité de données écrasées par une opération PutObject à partir du stockage S3 One Zone-IA
region1-*region2*-S3RTC-In-Bytes	Go	Mensuel	Quantité de données transférées pour le contrôle du temps de réplication S3 (S3 RTC) de *region2* vers *region1* par les opérationsPutObject ReplTime , GetObject ReplTime , InitiateMultipartUploadReplTime , UploadPartReplTime , CompleteMultipartUploadReplTime et WriteACLReplTime

Type d'utilisation	Unités	Granularité	Description
region1-*region2*-S3RTC-Out-Bytes	Go	Mensuel	Quantité de données transférées pour le contrôle du temps de réplication S3 (S3 RTC) de *region1* vers *region2* par les opérations PutObjectReplTime, GetObjectReplTime, InitiateMultipartUploadReplTime, UploadPartReplTime, CompleteMultipartUploadReplTime et WriteACLReplTime
region-Requests-GDA-Tier1	Nombre	Par heure	Nombre de demandes PUT, COPY, POST, CreateMultipartUpload, UploadPart ou CompleteMultipartUpload sur les objets S3 Glacier Deep Archive [6]
region-Requests-GDA-Tier2	Nombre	Par heure	Nombre de demandes GET et HEAD sur les objets S3 Glacier Deep Archive
region-Requests-GDA-Tier3	Nombre	Par heure	Nombre de demandes de restauration standard S3 Glacier Deep Archive

Type d'utilisation	Unités	Granularité	Description
region-Requests-GDA-Tier5	Nombre	Par heure	Nombre de demandes de restauration S3 Glacier Deep Archive en bloc
region-Requests-GIR-Tier1	Nombre	Par heure	Nombre de demandes PUT, COPY ou POST sur les objets S3 Glacier Instant Retrieval.
region-Requests-GIR-Tier2	Nombre	Par heure	Nombre de demandes GET et de toutes les autres demandes non-S3 Glacier Instant Retrieval -Tier1 sur les objets S3 Glacier Instant Retrieval
region-Requests-GLACIER-Tier1	Nombre	Par heure	Nombre de demandes PUT, COPY, POST, CreateMultipartUpload , UploadPart ou CompleteMultipartUpload sur les objets S3 Glacier Flexible Retrieval [6]
region-Requests-GLACIER-Tier2	Nombre	Par heure	Nombre de demandes GET et de toutes les autres demandes non répertoriées sur les objets S3 Glacier Flexible Retrieval
region-Requests-INT-Tier1	Nombre	Par heure	Nombre de demandes PUT, COPY ou POST portant sur les objets S3 Intelligent-Tiering

Type d'utilisation	Unités	Granularité	Description
region-Requests-INT-Tier2	Nombre	Par heure	Nombre des demandes GET et de toutes les autres demandes non-Tier1 portant sur les objets S3 Intelligent-Tiering
region-Requests-SIA-Tier1	Nombre	Par heure	Nombre de demandes PUT, COPY ou POST portant sur les objets S3 Standard-IA
region-Requests-SIA-Tier2	Nombre	Par heure	Nombre de demandes GET et de toutes les autres demandes non-S3 Glacier Instant Retrieval -Tier1 portant sur les objets S3 Standard-IA
region-Requests-Tier1	Nombre	Par heure	Nombre de demandes PUT, COPY ou POST pour S3 Standard, RRS et les balises, plus les demandes LIST pour tous les compartiments et les objets
region-Requests-Tier2	Nombre	Par heure	Nombre des demandes GET et de toutes les autres demandes non-Tier1

Type d'utilisation	Unités	Granularité	Description
region-Requests-Tier3	Nombre	Par heure	Nombre de demandes de cycle de vie envoyées à S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive et de demandes de restauration standard S3 Glacier Flexible Retrieval
region-Requests-Tier4	Nombre	Par heure	Nombre de transitions du cycle de vie vers le stockage S3 Glacier Instant Retrieval, S3 Intelligent-Tiering, S3 Standard-IA ou S3 One Zone-IA
region-Requests-Tier5	Nombre	Par heure	Nombre de demandes de restauration S3 Glacier Flexible Retrieval en bloc
region-Requests-Tier6	Nombre	Par heure	Nombre de demandes de restauration S3 Glacier Flexible Retrieval accélérées
region-Requests-Tier8	Nombre	Par heure	Nombre de demandes d'autorisations d'accès S3
region-Requests-XZ-Tier1	Nombre	Par heure	Nombre de demandes PUT ou COPY portant sur les objets S3 Express One Zone

Type d'utilisation	Unités	Granularité	Description
region-Requests-XZ-Tier2	Nombre	Par heure	Nombre de demandes GET et de toutes les autres demandes non-S3 Express One Zone-Tier 1 portant sur les objets S3 Express One Zone
region-Requests-ZIA-Tier1	Nombre	Par heure	Nombre de demandes PUT, COPY ou POST portant sur les objets S3 One Zone-IA
region-Requests-ZIA-Tier2	Nombre	Par heure	Le nombre de demandes non liées à S3 One Zone-IA-Tier 1 GET et toutes les autres requêtes sur des objets S3 One Zone-IA
region-Retrieval-GIR	Go	Par heure	Volume de données extraites du stockage S3 Glacier Instant Retrieval
region-Retrieval-SIA	Go	Par heure	Volume de données extraites du stockage S3 standard – Accès peu fréquent
region-Retrieval-XZ	Go	Par heure	Partie des données qui dépasse 512 Ko dans une demande de récupération donnée (PUT ou COPY) avec le stockage S3 Express One Zone

Type d'utilisation	Unités	Granularité	Description
region-Retrieval-ZIA	Go	Par heure	Volume de données extraites du stockage S3 One Zone-IA
region-S3DSSE-In-Bytes	Go	Mensuel	Quantité de données à double chiffrement par Amazon S3
region-S3DSSE-Out-Bytes	Go	Mensuel	Quantité de données à double chiffreme nt déchiffrées par Amazon S3
region-S3G-DataTransfer-In-Bytes	Go	Par heure	Volume de données transférées vers Amazon S3 pour restaurer des objets à partir d'un espace de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive
region-S3G-DataTransfer-Out-Bytes	Go	Par heure	Volume de données transférées depuis Amazon S3 pour transmettre des objets vers un espace de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive

Type d'utilisation	Unités	Granularité	Description
region-Select-Returned-Bytes	Go	Par heure	Volume de données retournées avec des demandes Select dans un stockage S3 Standard
region-Select-Returned-GIR-Bytes	Go	Par heure	Volume de données retournées avec des demandes Select du stockage S3 Glacier Instant Retrieval
region-Select-Returned-INT-Bytes	Go	Par heure	Volume de données retournées avec des demandes Select dans un stockage S3 Intelligent-Tiering
region-Select-Returned-SIA-Bytes	Go	Par heure	Volume de données retournées avec des demandes Select dans un stockage S3 standard – Accès peu fréquent
region-Select-Returned-ZIA-Bytes	Go	Par heure	Volume de données retournées avec des demandes Select dans un stockage S3 One Zone-IA
region-Select-Scanned-Bytes	Go	Par heure	Volume de données analysées avec des demandes Select dans un stockage S3 Standard

Type d'utilisation	Unités	Granularité	Description
region-Select-Scanned-GIR-Bytes	Go	Par heure	Volume de données analysées avec des demandes Select du stockage S3 Glacier Instant Retrieval
region-Select-Scanned-INT-Bytes	Go	Par heure	Volume de données analysées avec les demandes Select d'un stockage S3 Intelligent-Tiering
region-Select-Scanned-SIA-Bytes	Go	Par heure	Volume de données analysées avec des demandes Select dans un stockage S3 Standard-IA
region-Select-Scanned-ZIA-Bytes	Go	Par heure	Volume de données analysées avec des demandes Select dans un stockage S3 One Zone-IA
region-Standard-Retrieval-Bytes	Go	Par heure	Volume de données extraites à l'aide de demandes S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive standard
region-StorageAnalytics-ObjCount	Objets	Par heure	Nombre d'objets uniques surveillés dans chaque configuration Analyse de classe de stockage.

Type d'utilisation	Unités	Granularité	Description
region-StorageLens-ObjCount	Objets	Chaque jour	Nombre d'objets uniques dans chaque tableau de bord S3 Storage Lens qui sont suivis par des métriques avancées et des recommandations S3 Storage Lens.
region-StorageLensFreeTier-ObjCount	Objets	Chaque jour	Nombre d'objets uniques dans chaque tableau de bord S3 Storage Lens qui sont suivis par des métriques d'utilisation S3 Storage Lens.
StorageObjectCount	Nombre	Chaque jour	Nombre d'objets stockés dans un compartiment donné
region-Tables-CompactedObjects	Objets	Par heure	Le nombre d'objets compactés dans les compartiments de table Amazon S3
region-Tables-MonitoredObjects	Objets	Par heure	Le nombre d'objets dans les compartiments de table Amazon S3
region-Tables-ProcessedBytes	Go	Par heure	La quantité de données traitées pour le compactage dans les compartiments de table Amazon S3

Type d'utilisation	Unités	Granularité	Description
region-Tables-Requests-Tier1	Nombre	Par heure	Le nombre de requêtes PUT sur les compartiments de table Amazon S3
region-Tables-Requests-Tier2	Nombre	Par heure	Le nombre de requêtes GET et de toutes les autres requêtes non de niveau 1 sur les compartiments de table Amazon S3
region-Tables-TimedStorage-ByteHrs	Go-mois	Chaque jour	Le nombre de Go/mois pendant lesquels les données ont été stockées dans des compartiments de table Amazon S3
region-TagStorage-TagHrs	Balise-heures	Chaque jour	Nombre total de balises sur l'ensemble des objets du compartiment, par heure
region-TimedStorage-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage S3 Standard
region-TimedStorage-GDA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage S3 Glacier Deep Archive
region-TimedStorage-GDA-Staging	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage intermédiaire S3 Glacier Deep Archive

Type d'utilisation	Unités	Granularité	Description
region-TimedStorage-GIR-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage S3 Glacier Instant Retrieval
region-TimedStorage-GIR-SmObjects	Go-mois	Chaque jour	Nombre de Go-mois de petits objets (inférieurs à 128 Ko) stockés dans le stockage S3 Glacier Instant Retrieval.
region-TimedStorage-GlacierByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage S3 Glacier Flexible Retrieval
region-TimedStorage-GlacierStaging	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage intermédiaire S3 Glacier Flexible Retrieval
region-TimedStorage-INT-FA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le niveau Accès fréquent du stockage S3 Intelligent-Tiering[5]
region-TimedStorage-INT-IA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le niveau Accès peu fréquent du stockage S3 Intelligent-Tiering

Type d'utilisation	Unités	Granularité	Description
region-TimedStorage-INT-AA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le niveau Archive Access du stockage S3 Intelligent-Tiering
region-TimedStorage-INT-AIA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le niveau Archive Instant Access du stockage S3 Intelligent-Tiering
region-TimedStorage-INT-DAA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le niveau Deep Archive Access du stockage S3 Intelligent-Tiering
region-TimedStorage-RRS-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage RRS (Reduced Redundancy Storage)
region-TimedStorage-SIA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage S3 Standard-IA
region-TimedStorage-SIA-SmObjects	Go-mois	Chaque jour	Nombre de Go-mois de petits objets (inférieurs à 128 Ko) stockés dans le stockage S3 Standard-IA[4]
region-TimedStorage-XZ-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage S3 Express One Zone

Type d'utilisation	Unités	Granularité	Description
region-TimedStorage-ZIA-ByteHrs	Go-mois	Chaque jour	Nombre de Go-mois de données stockées dans le stockage S3 One Zone-IA
region-TimedStorage-ZIA-SmObjects	Go-mois	Chaque jour	Nombre de Go-mois de petits objets (inférieurs à 128 Ko) stockés dans le stockage S3 One Zone-IA
region-Upload-XZ	Go	Par heure	Quantité de données dépassant 512 Ko dans une demande de chargement donnée (PUT ou COPY) avec S3 Express One Zone

Remarques

1. Les types `Global-Bucket-Hrs-FreeTier` d'utilisation `Global-Bucket-Hrs` et les types d'utilisation s'appliquent aux seaux à usage général dans les applications commerciales Régions AWS et AWS GovCloud (US).
2. Si vous interrompez un transfert avant qu'il ne soit terminé, la quantité de données transférée peut dépasser la quantité de données que votre application reçoit. Cet écart peut survenir si une demande d'arrêt de transfert ne peut pas être exécutée instantanément et qu'une certaine quantité de données en transit est en attente de l'exécution de la demande de terminaison. Ces données en transit sont facturées comme données transférées « depuis ».
3. Pour les objets archivés dans les classes de stockage S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive qui sont supprimés, remplacés ou transférés avant leur période minimale d'engagement de stockage (90 jours pour S3 Glacier Instant Retrieval et S3 Glacier Flexible Retrieval, 180 jours pour S3 Glacier Deep Archive), des frais proportionnels par gigaoctet s'appliquent pour les jours restants. Ces frais sont reflétés sous forme de `EarlyDelete-GIREarlyDelete-ByteHrs`, et de types `EarlyDelete-GDA` d'utilisation respectivement sur votre facture.

4. Si des objets enregistrés dans le stockage S3 Standard-IA ou S3 One Zone-IA sont supprimés, écrasés ou transférés vers une autre classe de stockage avant 30 jours, des frais sont facturés au prorata par gigaoctet pour les jours restants.
5. Si de petits objets (inférieurs à 128 Ko) enregistrés dans le stockage S3 Standard-IA ou S3 One Zone-IA sont supprimés, écrasés ou transférés vers une autre classe de stockage avant 30 jours, des frais sont facturés au prorata par gigaoctet pour les jours restants.
6. Il n'existe pas de taille d'objet facturable minimale pour les objets de la classe de stockage S3 Intelligent-Tiering. Les objets dont la taille est inférieure à 128 Ko ne sont pas surveillés ni admissibles à la hiérarchisation automatique. Les objets plus petits sont stockés dans S3 Intelligent-Tiering – Accès fréquent.
7. Lorsque vous lancez une demande `CreateMultipartUpload`, `UploadPart` ou `UploadPartCopy` vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, les demandes sont facturées aux tarifs des demandes S3 Standard jusqu'à ce que vous ayez terminé le chargement partitionné. Une fois le chargement terminé, la demande `CompleteMultipartUpload` unique est facturée au tarif `PUT` du stockage S3 Glacier de destination. Les parties d'un chargement partitionné en cours d'exécution d'une commande `PUT` vers la classe de stockage S3 Glacier Flexible Retrieval sont facturées en tant que stockage de transit S3 Glacier Flexible Retrieval aux tarifs de stockage S3 Standard jusqu'à ce que le chargement soit terminé. De même, les parties d'un chargement partitionné en cours d'exécution d'une commande `PUT` vers la classe de stockage S3 Glacier Deep Archive sont facturées en tant que stockage de transit S3 Glacier Deep Archive aux tarifs de stockage S3 Standard jusqu'à ce que le chargement soit terminé.
8. S3 Express One Zone applique des frais fixes par demande pour les demandes d'une taille allant jusqu'à 512 Ko. Des frais supplémentaires par Go sont appliqués pour les demandes `PUT` et `GET` pour la partie de demande qui dépasse 512 Ko.
9. Pour plus d'informations sur les fonctionnalités prises en charge pour la classe de stockage S3 Express One Zone, consultez Fonctionnalités Amazon S3 non prises en charge par les compartiments de répertoires .
10. Les types d'utilisation dont les unités sont facturées en Go sont calculés en octets dans les rapports d'utilisation.
11. Un Go-mois est obtenu en prenant le nombre total de Go-heures, en les agrégeant tout au long d'un mois, puis en les divisant par le nombre d'heures dans le mois en question. Pour plus d'informations, consultez Questions fréquentes (FAQ) : Comment mon utilisation d'Amazon S3 m'est-elle facturée ?

> **Note**
>
> En général, les propriétaires de compartiments S3 se voient facturer les demandes comportant des réponses positives HTTP `200 OK` et des réponses d'erreur client HTTP `4XX`. Les propriétaires de compartiments ne se voient pas facturer les réponses d'erreur de serveur HTTP `5XX`, telles que les erreurs HTTP `503 Slow Down`. Pour plus d'informations sur les codes d'erreur S3 sous les codes de statut HTTP `3XX` et `4XX` non facturés, consultez Facturation des réponses d'erreur Amazon S3. Pour plus d'informations sur les frais de facturation si votre compartiment est configuré en tant que compartiment de type Paiement par le demandeur, consultez Fonctionnement du Paiement par le demandeur.

Opérations de suivi dans vos rapports d'utilisation

Les opérations décrivent l'action entreprise sur votre AWS objet ou compartiment par le type d'utilisation spécifié. Les opérations sont indiquées par des codes explicites comme `PutObject` ou `ListBucket`. Pour savoir quelles actions prises sur votre compartiment ont généré un type d'utilisation spécifique, utilisez ces codes. Lorsque vous générez un rapport d'utilisation, vous pouvez baser votre rapport sur toutes les opérations ou sur une opération en particulier comme `GetObject`.

Plus d'informations

- AWS rapports d'utilisation pour Amazon S3
- AWS Billing rapports pour Amazon S3
- Tarification Amazon S3
- Amazon S3 FAQs

Facturation des réponses d'erreur Amazon S3

En général, les propriétaires de compartiments S3 se voient facturer les demandes comportant des réponses positives HTTP `200 OK` et des réponses d'erreur client HTTP `4XX`. Les propriétaires de compartiments ne se voient pas facturer les réponses d'erreur de serveur HTTP `5XX`, telles que les erreurs HTTP `503 Slow Down`. Pour plus d'informations sur les frais de facturation si votre compartiment est configuré en tant que compartiment de type Paiement par le demandeur, consultez Fonctionnement du Paiement par le demandeur.

Le tableau suivant répertorie les codes d'erreur spécifiques sous les codes de statut HTTP 3XX et 4XX qui ne sont pas facturés. Pour les compartiments configurés avec l'hébergement de site Web, les frais de demande et autres frais applicables continueront de s'appliquer lorsque S3 renvoie un document d'erreur personnalisé ou pour les redirections personnalisées.

> **Note**
>
> Pour `AccessDenied` (HTTP`403 Forbidden`), S3 ne facture pas le propriétaire du compartiment lorsque la demande est initiée en dehors du AWS compte individuel du propriétaire du compartiment ou de l' AWS organisation du propriétaire du compartiment.

Code de statut HTTP	Code d'erreur	Description du code d'erreur
301 – Déplacé de façon permanente	PermanentRedirect	Le compartiment auquel vous tentez d'accéder doit être adressé à l'aide du point de terminaison spécifié. Envoyez toutes les demandes futures à ce point de terminaison.
	PermanentRedirectControlError	L'opération d'API à laquelle vous tentez d'accéder doit être adressée à l'aide du point de terminaison spécifié. Envoyez toutes les demandes futures à ce point de terminaison.
307 – Redirection temporaire	TemporaryRedirect	Vous êtes redirigé vers le compartiment pendant la mise à jour du serveur

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
		du système de nom de domaine (DNS).	
400 Requête erronée	AuthorizationHeaderMalformed	L'en-tête d'autorisation que vous avez fourni n'est pas valide.	
	AuthorizationQueryParametersError	Les paramètres de requête d'autorisation que vous avez fournis ne sont pas valides.	
	ConnectionClosedByRequester	Renvoyé à l'appelant d'origine lorsqu'une erreur survient lors de la lecture du WriteGetObjectResponse corps du message.	
	DeviceNotActiveError	L'appareil n'est actuellement pas actif.	
	EndpointNotFound	Dirigez les demandes vers le point de terminaison approprié.	
	ExpiredToken	Le jeton fourni a expiré.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	IllegalLocationConstraintException	Vous essayez d'accéder à un compartiment depuis une région différente de celle où le compartiment existe. Pour éviter cette erreur, utilisez l'option `--region`. Par exemple : `aws s3 cp` *`awsexample.txt`* `s3://` *`amzn-s3-demo-bucket`* `/ --region` *`ap-east-1`* .	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	InvalidArgument	Cette erreur peut se produire dans les conditions suivantes : • L'argument spécifié n'était pas valide. • Il manquait un en-tête obligatoire à la demande. • L'argument spécifié était incomplet ou n'était pas au bon format. • L'argument spécifié doit avoir une longueur supérieure ou égale à 3.	
	InvalidBucketOwnerAWSAccountID	La valeur du paramètre attendu pour le propriétaire du compartiment doit être un Compte AWS ID.	
	InvalidDigest	La valeur de contenu MD5 ou de somme de contrôle que vous avez spécifiée n'est pas valide.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	InvalidEncryptionAlgorithmError	La demande de chiffrement que vous avez spécifiée n'est pas valide. La valeur valide est AES256.	
	InvalidHostHeader	Les en-têtes d'hôte fournis dans la demande utilisaient un style d'adressage incorrect.	
	InvalidHttpMethod	La demande est effectuée à l'aide d'une méthode HTTP inattendue.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	InvalidRequest	Cette erreur peut se produire dans les conditions suivantes : • La version de signature utilisée dans la demande est incorrecte. Utilisez `AWS4-HMAC-SHA256` (Signature Version 4). • Un point d'accès ne peut être créé que pour un compartiment existant. • Le point d'accès n'est pas dans un état où il peut être supprimé. • Un point d'accès ne peut être répertorié que pour un compartiment existant. • Le jeton suivant n'est pas valide. • Au moins une action doit être spécifiée dans une règle du cycle de vie. •	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
		Au moins une règle du cycle de vie doit être spécifiée. • Le nombre de règles du cycle de vie ne doit pas dépasser la limite autorisée de 1 000 règles. • La plage pour le paramètre `MaxResults` n'est pas valide. • Les demandes SOAP doivent être effectuées via une connexion HTTPS. • Amazon S3 Transfer Acceleration n'est pas pris en charge pour les compartiments dont les noms ne sont pas conformes à DNS. • Amazon S3 Transfer Acceleration n'est pas pris en charge pour les compartiments dont le nom contient des points (.). •	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
		Le point de terminaison Amazon S3 Transfer Acceleration ne prend en charge que les demandes de style virtuelles. • Amazon S3 Transfer Acceleration n'est pas configuré sur ce compartiment. • Amazon S3 Transfer Acceleration est désactivé sur ce compartiment. • Amazon S3 Transfer Acceleration n'est pas pris en charge sur ce compartiment. Pour obtenir de l'aide, contactez Support. • Amazon S3 Transfer Acceleration ne peut pas être activé sur ce compartiment. Pour obtenir de l'aide, contactez Support. • Valeurs contradictoires fournies dans les	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
		en-têtes HTTP et les paramètres de requête. • Valeurs contradictoires fournies dans les en-têtes HTTP et les champs de formulaire POST. • CopyObject demande effectuée sur des objets d'une taille supérieure à 5 Go.	
	InvalidSessionException	Renvoyé si la session n'existe plus après avoir expiré.	
	InvalidSignature	La signature de demande que le serveur a calculée ne correspond pas à la signature que vous avez fournie. Vérifiez votre clé d'accès AWS secrète et votre méthode de signature. Pour plus d'informations, consultez Signature et authentification des demandes REST.	
	Non valide SOAPRequest	Le corps de la demande SOAP n'est pas valide.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	InvalidStorageClass	La classe de stockage que vous avez spécifiée n'est pas valide.	
	InvalidTag	Votre demande contient une entrée de balise qui n'est pas valide. Par exemple, votre demande peut contenir des clés dupliquées, des clés ou des valeurs trop longues ou des balises système.	
	InvalidToken	Le jeton fourni est mal formé ou n'est pas valide.	
	InvalidURI	L'URI spécifié n'a pas pu être analysé.	
	KeyTooLongError	Votre clé est trop longue.	
	KM. DisabledException	La demande a été rejetée, car la clé KMS spécifiée n'est pas activée.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	KM. InvalidKeyUsageException	Cette demande a été rejetée pour l'une des raisons suivantes : • La KeyUsage valeur de la clé KMS est incompatible avec le fonctionnement de l'API. • L'algorithme de chiffrement ou de signature spécifié pour l'opération est incompatible avec le type de contenu clé de la clé KMS (KeySpec). Pour le chiffrement, le déchiffrement, le rechiffrement et la génération de clés de données, le code doit être ENCRYPT_DECRYPT. KeyUsage Pour signer et vérifier les messages, le nom KeyUsage doit être SIGN_VERIFY. Pour générer et vérifier les codes d'authentification des messages (MACs), le code KeyUsage doit être GENERATE_	

Code de statut HTTP	Code d’erreur	Description du code d’erreur	
		VERIFY_MAC. Pour obtenir les principaux secrets d'un accord, le code KeyUsage doit être KEY_AGREEMENT. Pour trouver KeyUsage une clé KMS, utilisez l' DescribeKey opération. Pour trouver les algorithmes de chiffrement ou de signature pris en charge pour une clé KMS spécifique, utilisez l' DescribeKey opération.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	KM. KMSInvalidStateException	La demande a été rejetée, car l'état de la ressource spécifiée n'est pas valide pour cette demande. Cette exception a l'une des significations suivantes : • L'état de clé de la clé KMS n'est pas compatible avec l'opération. Pour trouver l'état clé, utilisez l' DescribeKey opération. Pour plus d'informations sur les états de clé compatibles avec chaque opération KMS, consultez États de clé de AWS KMS keys dans le Guide du développeur AWS Key Management Service . • Pour les opérations cryptographiques sur les clés KMS dans les magasins de clés personnalisés, cette exception représente un échec général avec de nombreuses causes	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
		possibles. Pour identifier la cause, consultez le message d'erreur qui accompagne l'exception.	
	KM. NotFoundException	La demande a été rejetée, car l'entité ou la ressource spécifiée est introuvable.	
	LambdaInvalidResponse	Renvoyé à l'appelant d'origine lorsqu'il WriteGetObjectResponse répond par « ValidationError à AWS Lambda ». Consultez le ValidationError message pour plus de détails. Tous les cas ne se ValidationError traduisent pas par une LambdaInvalidResponse erreur.	

Code de statut HTTP	Code d’erreur	Description du code d’erreur	
	LambdaInvocationFailed	L’invocation de la fonction Lambda a échoué. Les appelants peuvent recevoir l’erreur suivante lorsque S3 Object Lambda ne parvient pas à invoquer correctem ent la fonction Lambda configurée. Le message d'erreur peut contenir des détails sur une éventuell e erreur renvoyée par le AWS Lambda service lors de l'appel de la fonction (par exemple, le code d'état, le code d'erreur, le message d'erreur et l'ID de demande).	
	Malformé ACLError	La liste ACL que vous avez fournie n’est pas bien formée ou n’a pas été validée par rapport à notre schéma publié.	
	Malformé POSTRequest	Le corps de votre demande POST n’est pas un multipart/form-data bien formé.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	MalformedXML	Le code XML que vous avez fourni n'est pas bien formé ou n'a pas été validé par rapport à notre schéma publié.	
	MaxPostPreDataLengthExceededError	Les champs de votre demande POST précédant le fichier de chargement étaient trop volumineux.	
	MetadataTooLarge	Vos en-têtes de métadonnées dépassent la taille de métadonnées maximale autorisée.	
	MissingAttachment	Une pièce jointe SOAP était attendue, mais aucune n'a été trouvée.	
	MissingRequestBodyError	Vous avez envoyé un document XML vide sous forme de demande.	
	MissingSecurityHeader	Il manque un en-tête obligatoire dans votre demande.	
	NoLoggingStatusForKey	Il n'existe pas de sous-ressource de statut de journalisation pour une clé.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	NotDeviceOwnerError	L'appareil qui a généré le jeton n'appartient pas à l'utilisateur authentifié.	
	ResponseInterrupted	Renvoyé à l'appelant d'origine lorsqu'une erreur survient lors de la lecture du WriteGetObjectResponse corps du message.	
	RequestHeaderSectionTooLarge	L'en-tête de demande et les paramètres de requête utilisés pour que la demande dépasse les tailles maximales autorisées	
	TokenCodeInvalidError	Le numéro de série et/ou le code de jeton que vous avez fournis ne sont pas valides.	
	UnexpectedContent	Cette demande contient du contenu non pris en charge.	
	UnsupportedArgument	La demande contenait un argument non pris en charge.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	UnsupportedSignature	La demande fournie est signée avec une version de jeton STS non prise en charge ou la version de signature n'est pas prise en charge.	
	UserKeyMustBeSpecified	La demande POST du compartiment doit contenir le nom de champ spécifié. S'il est spécifié, vérifiez l'ordre des champs.	
	IncorrectEndpoint	Le compartiment spécifié existe dans une autre région. Dirigez les demandes vers le point de terminaison approprié.	
	ValidationError	Des erreurs de validation peuvent être renvoyées par le fonctionnement de l' WriteGetObjectResponse API et peuvent se produire pour de nombreuses raisons. Consultez le message d'erreur pour plus de détails.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
403 Forbidden	RequestTimeTooSkewed	La différence entre l'heure de la demande et celle du serveur est trop importante.	
	SignatureDoesNotMatch	La signature de demande que le serveur a calculée ne correspond pas à la signature que vous avez fournie. Vérifiez votre clé d'accès AWS secrète et votre méthode de signature. Pour plus d'informations, consultez Authentification REST et Authentification SOAP.	
	NotSignedUp	Votre compte n'est pas inscrit pour le service Amazon S3. Vous devez vous inscrire avant de pouvoir utiliser Amazon S3. Vous pouvez vous inscrire à l'adresse suivante : https://aws.amazon.com/s3	
	InvalidSecurity	Les informations d'identification de sécurité fournies ne sont pas valides.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	InvalidPayer	Tous les accès à cet objet ont été désactivé s. Pour obtenir de l'aide, consultez Contactez-nous.	
	InvalidAccessKeyId	L'identifiant de clé d' AWS accès que vous avez fourni n'existe pas dans nos dossiers.	
	AccountProblem	Il y a un problème avec votre Compte AWS appareil qui empêche l'opération de se terminer correctement. Pour obtenir de l'aide, consultez Contactez-nous.	
	UnauthorizedAccessError	Applicable dans les régions de Chine uniquement. Renvoyé lorsqu'une demande est adressée à un compartim ent qui ne possède pas de licence ICP. Pour plus d'informations, consultez Enregistrement ICP.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	Inattendu IPError	Applicable dans les régions de Chine uniquement. Cette demande a été rejetée, car l'adresse IP était inattendue.	
	MissingAuthenticationToken	La demande n'a pas été signée.	
	LambdaPermissionError	L'appelant n'est pas autorisé à invoquer la fonction Lambda. L'appelant doit être autorisé à invoquer la fonction Lambda. Vérifiez les politiques associées à l'appelant et assurez-vous qu'elles ont été autorisées à utiliser `lambda:Invoke` pour la fonction configurée. Le message d'erreur peut contenir des détails sur une erreur éventuelle renvoyée par le service Lambda lors de l'invocation de la fonction (par exemple, le code de statut, le code d'erreur, le message d'erreur et l'ID de demande).	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
404 – Non trouvé	LambdaNotFound	La AWS Lambda fonction n'a pas été trouvée. La fonction, la version ou l'alias Lambda configurés n'ont pas été trouvés lors de la tentative d'invocation. Veillez à ce que la configuration du point d'accès S3 Object Lambda pointe vers l'ARN correct de la fonction Lambda. Le message d'erreur peut contenir des détails sur une éventuelle erreur renvoyée par le AWS Lambda service lors de l'appel de la fonction (par exemple, le code d'état, le code d'erreur, le message d'erreur et l'ID de demande).	
	NoSuchAsyncRequest	La demande spécifiée est introuvable.	
	NoSuchObjectLockConfiguration	L'objet spécifié n'a pas de ObjectLock configuration.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
	NoSuchUpload	Le chargement partitionné spécifié n'existe pas. L'ID de chargement n'est peut-être pas valide ou le chargement partitionné a peut-être été abandonné ou terminé.	
	NoSuchWebsiteConfiguration	Le compartiment spécifié n'a aucune configuration de site Web.	
	NoTransformationDefined	Aucune transformation n'a été trouvée pour ce point d'accès Object Lambda.	
	ObjectLockConfigurationNotFoundError	La configuration de verrouillage d'objet n'existe pas pour ce compartiment.	
405 – Méthode non autorisée	MethodNotAllowed	La méthode spécifiée n'est pas autorisée sur cette ressource.	

Code de statut HTTP	Code d'erreur	Description du code d'erreur	
409 – Conflit	BucketAlreadyExists	Le nom de compartiment demandé n'est pas disponible. L'espace de noms de compartiments est partagé par tous les utilisateurs du système. Spécifiez un nom différent et réessayez.	
	InvalidBucketState	La demande n'est pas valide pour l'état actuel du compartiment.	
	OperationAborted	Une opération conditionnelle conflictuelle est actuellement en cours sur cette ressource. Réessayez.	
411 – Longueur requise	MissingContentLength	Vous devez fournir l'en-tête HTTP Content-Length.	
412 – Échec de condition préalable	RequestIsNotMultiPartContent	Une demande POST de compartiment doit être du type d'encadrement multipart/form-data.	
416 – Plage demandée impossible à respecter	InvalidRange	La plage demandée n'est pas valide pour la demande. Essayez d'utiliser une autre plage.	

Bien comprendre et gérer les classes de stockage Amazon S3

Dans Simple Storage Service (Amazon S3), chaque objet possède une classe de stockage qui lui est associée. Par défaut, les objets figurant dans S3 sont stockés dans la classe de stockage S3 Standard, mais Amazon S3 offre toute une gamme d'autres classes de stockage pour vos objets. Vous choisissez une classe de stockage en fonction du cas d'utilisation et des exigences en matière de performances d'accès. Le choix d'une classe de stockage adaptée à votre cas d'utilisation vous permet d'optimiser les coûts, les performances et la disponibilité du stockage de vos objets. Toutes ces classes de stockage offrent une durabilité élevée.

Les sections suivantes fournissent des détails sur les différentes classes de stockage et vous expliquent comment définir une classe de stockage pour vos objets.

Rubriques

- Classes de stockage pour les objets fréquemment consultés
- Classe de stockage pour l'optimisation automatique des données avec des modèles d'accès inconnus ou irréguliers
- Classes de stockage pour les objets à accès peu fréquent
- Classes de stockage pour les objets rarement consultés
- Classe de stockage pour Amazon S3 sur Outposts
- Comparaison des classes de stockage Amazon S3
- Définition de la classe de stockage d'un objet
- Analyses Amazon S3 - Analyse de classe de stockage
- Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering
- Présentation des classes de stockage S3 Glacier pour le stockage de données à long terme
- Utilisation des objets archivés

Classes de stockage pour les objets fréquemment consultés

Pour les cas d'utilisation sensibles aux performances (requérant des temps d'accès de l'ordre de la milliseconde) et les données fréquemment consultées, Simple Storage Service (Amazon S3) fournit les classes de stockage suivantes :

- S3 Standard (`STANDARD`) : classe de stockage par défaut. Si vous ne spécifiez pas la classe de stockage lors du chargement d'un objet, Simple Storage Service (Amazon S3) affecte la classe de

stockage S3 Standard. Pour mieux optimiser les coûts entre S3 Standard et S3 Standard-IA, vous pouvez utiliser Analyses Amazon S3 - Analyse de classe de stockage.

- S3 Express One Zone (`EXPRESS_ONEZONE`) — Amazon S3 Express One Zone est une classe de stockage Amazon S3 à zone unique à hautes performances, spécialement conçue pour fournir un accès aux données cohérent à un chiffre en millisecondes à un chiffre pour vos applications les plus sensibles à la latence. S3 Express One Zone est la classe de stockage d'objets cloud qui présente la latence la plus faible à l'heure actuelle, avec une vitesse d'accès aux données jusqu'à 10 fois plus grande et des coûts de demande 50 % inférieurs à ceux de S3 Standard. Avec S3 Express One Zone, vos données sont stockées de façon redondante sur plusieurs appareils au sein d'une même zone de disponibilité. Pour de plus amples informations, veuillez consulter S3 Express One Zone.
- Stockage à redondance réduite (**`REDUCED_REDUNDANCY`**) : la classe de stockage à redondance réduite (RRS) est conçue pour les données non critiques et reproductibles qui peuvent être stockées avec moins de redondance que la classe de stockage standard S3.

  > **Important**
  >
  > Nous vous recommandons de ne pas utiliser cette classe de stockage. La classe de stockage S3 Standard est plus économique.

  En matière de durabilité, les objets RRS présentent une perte moyenne annuelle de 0,01 % d'objets. Si un objet RRS est perdu, lorsque des demandes sont effectuées sur cet objet, Simple Storage Service (Amazon S3) renvoie une erreur 405.

Classe de stockage pour l'optimisation automatique des données avec des modèles d'accès inconnus ou irréguliers

S3 Intelligent-Tiering (`INTELLIGENT_TIERING`) est une classe de stockage Amazon S3 conçue pour optimiser les coûts de stockage en déplaçant automatiquement les données vers le niveau d'accès le plus rentable, sans impact sur les performances ni surcharge opérationnelle. S3 Intelligent-Tiering est la seule classe de stockage dans le cloud qui permet de réaliser automatiquement des économies en déplaçant les données à un niveau d'objet granulaire entre les niveaux d'accès lorsque les modèles d'accès changent. S3 Intelligent-Tiering est la classe de stockage idéale si vous souhaitez optimiser vos coûts de stockage pour les données dont les modèles d'accès sont inconnus ou variables. L'utilisation de la classe S3 Intelligent-Tiering n'implique aucuns frais de récupération.

Moyennant des frais mensuels minimes de surveillance et d'automatisation des objets, S3 Intelligent-Tiering surveille les schémas d'accès et déplace automatiquement les objets qui n'ont pas été consultés vers des niveaux d'accès moins coûteux. S3 Intelligent-Tiering permet de réduire automatiquement les coûts de stockage grâce à trois niveaux d'accès à faible latence et à haut débit. Pour les données accessibles de manière asynchrone, vous pouvez choisir d'activer les capacités d'archivage automatique dans la classe de stockage S3 Intelligent-Tiering. S3 Intelligent-Tiering est conçue pour une disponibilité de 99,9 % et une durabilité de 99,999999999 %.

S3 Intelligent-Tiering stocke automatiquement les objets dans trois niveaux d'accès :

- Accès fréquent : les objets chargés ou migrés dans S3 Intelligent-Tiering sont stockés automatiquement au niveau Accès fréquent.
- Accès peu fréquent : S3 Intelligent-Tiering déplace vers le niveau Accès peu fréquent les objets qui n'ont pas été consultés pendant 30 jours consécutifs.
- Accès Archive Instant : avec S3 Intelligent-Tiering, tous les objets existants qui n'ont pas été consultés pendant 90 jours consécutifs sont automatiquement transférés vers le niveau d'accès Archive Instant.

Outre ces trois niveaux, S3 Intelligent-Tiering propose deux niveaux d'accès d'archive en option :

- Accès Archive : S3 Intelligent-Tiering vous offre la possibilité d'activer le niveau d'accès Archive pour les données accessibles de manière asynchrone. Une fois activé, le niveau d'accès Archive archive automatiquement les objets qui n'ont pas été consultés pendant un minimum de 90 jours consécutifs.
- Accès Deep Archive : S3 Intelligent-Tiering vous offre la possibilité d'activer le niveau d'accès Deep Archive pour les données accessibles de manière asynchrone. Une fois activé, le niveau d'accès Deep Archive archive automatiquement les objets qui n'ont pas été consultés pendant un minimum de 180 jours consécutifs.

> **Note**
>
> - N'activez le niveau d'accès Archive que pendant 90 jours si vous souhaitez contourner le niveau d'accès Archive Instant. Le niveau Archive Access permet de réduire légèrement les coûts de stockage et les délais de minute-to-hour récupération. Le niveau d'accès Archive Instant offre un accès de l'ordre de la milliseconde et des performances à haut débit.

- Activez les niveaux d'accès Archive et Deep Archive uniquement si vos objets sont accessibles de manière asynchrone par votre application. Si l'objet que vous récupérez est stocké au niveau d'accès Archive ou Deep Archive, restaurez d'abord l'objet à l'aide de `RestoreObject`.

Vous pouvez déplacer les données récemment créées vers S3 Intelligent-Tiering en le définissant comme classe de stockage par défaut. Vous pouvez également choisir d'activer l'un ou les deux niveaux d'accès aux archives à l'aide de l'opération `PutBucketIntelligentTieringConfiguration`API, de la AWS CLI console Amazon S3 ou des deux. Pour plus d'informations sur l'utilisation de S3 Intelligent-Tiering et sur l'activation des niveaux d'accès d'archive, consultez Utiliser S3 Intelligent-Tiering.

Pour accéder à des objets aux niveaux Archive Access ou Deep Archive Access, vous devez d'abord les restaurer. Pour plus d'informations, consultez Restauration des objets à partir des niveaux d'accès Archive et Deep Archive de S3 Intelligent-Tiering.

> **Note**
>
> Si la taille d'un objet est inférieure à 128 Ko, il ne sera pas admissible à la hiérarchisation automatique. Les objets plus petits sont toujours stockés dans le niveau Accès fréquent. Pour plus d'informations sur S3 Intelligent-Tiering, consultez Niveaux d'accès S3 Intelligent-Tiering..

Classes de stockage pour les objets à accès peu fréquent

Les classes de stockage S3 Standard-IA et S3 One Zone-IA sont conçues pour des données à longue durée de vie et à accès peu fréquent. (IA correspond à « Infrequent Access » [Accès peu fréquent].) Les objets S3 Standard-IA et S3 One Zone-IA sont disponibles avec un temps d'accès de l'ordre de la milliseconde (comme la classe de stockage S3 Standard). Simple Storage Service (Amazon S3) facture des frais de récupération pour ces objets. Ils sont donc plus adaptés aux données à accès peu fréquent. Pour en savoir plus sur la tarification, consultez Tarification Amazon S3.

Par exemple, vous pouvez choisir les classes de stockage S3 Standard-IA et S3 One Zone-IA pour les utilisations suivantes :

- Pour le stockage des sauvegardes.
- Pour des données anciennes qui sont rarement consultées, mais qui requièrent encore des temps d'accès de l'ordre de la milliseconde. Par exemple, lorsque vous chargez des données, vous pouvez choisir la classe de stockage S3 standard et utiliser la configuration du cycle de vie pour indiquer à Simple Storage Service (Amazon S3) de faire passer les objets vers la classe S3 Standard-IA ou S3 One Zone-IA.

  Pour plus d'informations sur la gestion du cycle de vie, consultez Gestion du cycle de vie des objets.

> **Note**
>
> Les classes de stockage S3 Standard-IA et S3 One Zone-IA sont adaptées pour les objets de plus de 128 Ko que vous envisagez de stocker pendant au moins 30 jours. Si un objet a une taille inférieure à 128 Ko, Amazon S3 vous facture 128 Ko. Si vous supprimez un objet avant la période minimale de stockage de 30 jours, les 30 jours vous sont facturés. Les objets supprimés, remplacés ou transférés dans une autre classe de stockage dans les 30 jours sont soumis aux frais d'utilisation normaux du stockage, auxquels s'ajoutent des frais calculés au prorata pour le reste de la période minimale de 30 jours. Pour en savoir plus sur la tarification, consultez Tarification Amazon S3.

Ces classes de stockage diffèrent sur les points suivants :

- S3 Standard-IA (`STANDARD_IA`) — Amazon S3 stocke les données des objets de manière redondante dans plusieurs zones de disponibilité géographiquement séparées (similaire à la classe de stockage S3 Standard). Les objets S3 standard – Accès peu fréquent résistent à la perte d'une zone de disponibilité. Cette classe de stockage offre plus de disponibilité et de résilience que la classe S3 One Zone-IA. Pour mieux optimiser les coûts entre S3 Standard et S3 Standard-IA, vous pouvez utiliser Analyses Amazon S3 - Analyse de classe de stockage.
- S3 One Zone-IA (`ONEZONE_IA`) — Amazon S3 stocke les données des objets dans une seule zone de disponibilité, ce qui les rend moins onéreuses que S3 Standard-IA. Toutefois, les données ne résistent pas à la perte physique de la zone de disponibilité suite à une catastrophe naturelle, telle qu'un séisme ou une inondation. La classe de stockage S3 One Zone-IA a la même durabilité que S3 Standard-IA, mais elle présente une disponibilité et une résilience moindres. Pour comparer la durabilité et la disponibilité des classes de stockage, consultez Comparaison des classes de stockage Amazon S3 à la fin de cette section. Pour en savoir plus sur la tarification,

consultez Tarification Amazon S3. Pour les cas d'utilisation liés à la résidence et à l'isolation des données, vous pouvez créer des compartiments de répertoire dans les zones AWS locales et utiliser les classes de stockage S3 Express One Zone (`EXPRESS_ONEZONE`) et S3 One Zone-IA (`ONEZONE_IA`). Pour plus d'informations sur les compartiments de répertoires dans les zones locales, consultez Charges de travail liées à la résidence des données.

Nous vous recommandons la procédure suivante :

- S3 Standard-IA (`STANDARD_IA`) — À utiliser pour votre copie principale ou unique de données qui ne peuvent pas être recréées.
- S3 One Zone-IA (`ONEZONE_IA`) — À utiliser si vous pouvez recréer les données en cas de défaillance de la zone de disponibilité, pour les répliques d'objets lors de la configuration de la réplication entre régions (CRR) S3. En outre, pour la résidence et l'isolation des données, vous pouvez créer des compartiments de répertoire dans les zones AWS locales et utiliser la classe de stockage S3 One Zone-IA.

Classes de stockage pour les objets rarement consultés

Les classes de stockage S3 Glacier Instant Retrieval (`GLACIER_IR`), S3 Glacier Flexible Retrieval (`GLACIER`) et S3 Glacier Deep Archive (`DEEP_ARCHIVE`) sont conçues pour le stockage et l'archivage des données à long terme et à faible coût. Ces classes de stockage nécessitent des durées de stockage minimales et induisent des frais de récupération minimum, ce qui les rend particulièrement efficaces pour les données rarement consultées. Pour plus d'informations sur les classes de stockage S3 Glacier, consultez Présentation des classes de stockage S3 Glacier pour le stockage de données à long terme.

Amazon S3 fournit les classes de stockage S3 Glacier suivantes :

- S3 Glacier Instant Retrieval (`GLACIER_IR`) : à utiliser pour les données à long terme rarement consultées et nécessitant une extraction en quelques millisecondes. Les données de cette classe de stockage sont disponibles pour un accès en temps réel.
- S3 Glacier Flexible Retrieval (`GLACIER`) — À utiliser pour les archives où certaines parties des données peuvent avoir besoin d'être récupérées en quelques minutes. Les données de cette classe de stockage sont archivées et ne sont pas disponibles pour un accès en temps réel.

- S3 Glacier Deep Archive (`DEEP_ARCHIVE`) : à utiliser pour archiver des données rarement accessibles. Les données de cette classe de stockage sont archivées et ne sont pas disponibles pour un accès en temps réel.

Récupération d'objets archivés

Vous pouvez définir la classe de stockage d'un objet sur S3 Glacier Flexible Retrieval (`GLACIER`) ou S3 Glacier Deep Archive (`DEEP_ARCHIVE`) de la même manière que pour les autres classes de stockage, comme décrit dans la sectionDéfinition de la classe de stockage d'un objet. Toutefois, les objets S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive sont archivés et ne sont pas disponibles pour un accès en temps réel. Pour de plus amples informations, veuillez consulter Présentation du stockage d'archivage dans S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.

> **Note**
>
> Lorsque vous utilisez les classes de stockage S3 Glacier, vos objets restent dans Amazon S3. Vous ne pouvez pas y accéder directement via le service Amazon S3 Glacier distinct. Pour obtenir des informations sur le service Amazon S3 Glacier, consultez le Guide du développeur Amazon S3 Glacier.

Classe de stockage pour Amazon S3 sur Outposts

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts ressources et stocker et récupérer des objets sur site pour les applications qui nécessitent un accès aux données locales, un traitement local des données et une résidence des données. Vous pouvez utiliser les mêmes opérations et fonctionnalités d'API AWS Outposts que sur Amazon S3, notamment les politiques d'accès, le chiffrement et le balisage. Vous pouvez utiliser S3 sur Outposts via l'API AWS Management Console, AWS CLI AWS SDKs, ou REST.

S3 sur Outposts fournit une nouvelle classe de stockage, S3 Outposts (`OUTPOSTS`). La classe de stockage S3 Outposts n'est disponible que pour les objets stockés dans des compartiments sur Outposts. Si vous essayez d'utiliser cette classe de stockage avec un compartiment S3 dans un Région AWS, une `InvalidStorageClass` erreur se produit. En outre, si vous essayez d'utiliser d'autres classes de stockage S3 avec des objets stockés dans S3 sur Outposts, la même réponse d'erreur se produit.

Les objets stockés dans la classe de stockage S3 Outposts (OUTPOSTS) sont toujours chiffrés à l'aide du chiffrement côté serveur avec les clés de chiffrement gérées par Amazon S3 (SSE-S3). Pour plus d'informations, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3).

Vous pouvez également choisir explicitement de chiffrer les objets stockés dans la classe de stockage S3 Outposts en utilisant le chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C). Pour de plus amples informations, veuillez consulter Utilisation du chiffrement côté serveur avec les clés fournies par le client (SSE-C).

> **Note**
>
> S3 on Outposts ne prend pas en charge le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS).

Pour plus d'informations sur S3 sur Outposts, consultez Qu'est-ce que S3 sur Outposts ? dans le Guide de l'utilisateur Amazon S3 sur Outposts.

Comparaison des classes de stockage Amazon S3

Le tableau suivant compare les classes de stockage, y compris leur disponibilité, leur durabilité, leur durée de stockage minimale et d'autres considérations.

Storage Class	Designed for	Durability (designed for)	Availability (designed for)	Availability Zones	Min storage duration	Min billable object size	Other Considerations
STANDARD	Frequently accessed data	99.999999999%	99.99%	>= 3	None	None	None
STANDARD_IA	Long-lived, infrequently accessed data	99.999999999%	99.9%	>= 3	30 days	128 KB	Per GB retrieval fees apply.
INTELLIGENT_TIERING	Long-lived data with changing or unknown access patterns	99.999999999%	99.9%	>= 3	30 days	None	Monitoring and automation fees per object apply. No retrieval fees.
ONEZONE_IA	Long-lived, infrequently accessed, non-critical data	99.999999999%	99.5%	1	30 days	128 KB	Per GB retrieval fees apply. Not resilient to the loss of the Availability Zone.
GLACIER	Long-term data archiving with retrieval times ranging from minutes to hours	99.999999999%	99.99% (after you restore objects)	>= 3	90 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects.
DEEP_ARCHIVE	Archiving rarely accessed data with a default retrieval time of 12 hours	99.999999999%	99.99% (after you restore objects)	>= 3	180 days	None	Per GB retrieval fees apply. You must first restore archived objects before you can access them. For more information, see Restoring Archived Objects.
RRS (Not recommended)	Frequently accessed, non-critical data	99.99%	99.99%	>= 3	None	None	None

* S3 Glacier Flexible Retrieval nécessite 40 Ko de métadonnées supplémentaires pour chaque objet archivé. Cela inclut 32 Ko de métadonnées facturés au tarif S3 Glacier Flexible Retrieval (requis pour identifier et récupérer vos données), et 8 Ko de données supplémentaires facturés au tarif S3 Standard. Le tarif S3 Standard est requis pour conserver le nom et les métadonnées définis par l'utilisateur pour les objets archivés dans S3 Glacier Flexible Retrieval. Pour plus d'informations sur les classes de stockage, consultez Classes de stockage Amazon S3.

** S3 Glacier Deep Archive nécessite 40 Ko de métadonnées supplémentaires pour chaque objet archivé. Cela inclut 32 Ko de métadonnées facturés au tarif S3 Glacier Deep Archive (requis pour identifier et récupérer vos données), et 8 Ko de données supplémentaires facturés au tarif S3 Standard. Le tarif S3 Standard est requis pour conserver le nom et les métadonnées définis par l'utilisateur pour les objets archivés dans Amazon S3 Glacier Deep Archive. Pour plus d'informations sur les classes de stockage, consultez Classes de stockage Amazon S3.

Sachez que toutes les classes de stockage, à l'exception de S3 One Zone-IA (`ONEZONE_IA`) et S3 Express One Zone (`EXPRESS_ONEZONE`), sont conçues pour résister à la perte physique d'une zone de disponibilité résultant de catastrophes. De plus, outre les performances requises par votre scénario d'application, tenez compte des coûts. Pour connaître les prix des classes de stockage, consultez Tarification Amazon S3.

Définition de la classe de stockage d'un objet

Vous pouvez spécifier une classe de stockage pour un objet lorsque vous le chargez. Si ce n'est pas le cas, Amazon S3 utilise la classe de stockage standard Amazon S3 par défaut pour les objets placés dans des compartiments à usage général. Vous pouvez également remplacer la classe de stockage d'un objet déjà stocké dans un compartiment à usage général Amazon S3 par une autre classe de stockage à l'aide de la console Amazon S3 ou du AWS Command Line Interface (AWS CLI). AWS SDKs Toutes ces approches utilisent les opérations d'API Amazon S3 pour envoyer des demandes à Amazon S3.

> **Note**
>
> Vous ne pouvez pas modifier la classe de stockage des objets stockés dans des compartiments de répertoire.

Vous pouvez indiquer à Amazon S3 de changer automatiquement la classe de stockage d'objets en ajoutant une configuration du cycle de vie S3 à un compartiment. Pour de plus amples informations, veuillez consulter Gestion du cycle de vie des objets.

Lors de la définition d'une configuration de réplication S3, vous pouvez définir la classe de stockage pour les objets répliqués sur n'importe quelle autre classe de stockage. Cependant, vous ne pouvez pas répliquer des objets stockés dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour de plus amples informations, veuillez consulter Éléments du fichier de configuration de réplication.

Lorsque vous définissez la classe de stockage par programmation, vous fournissez la valeur de la classe de stockage. Voici la liste des noms de consoles pour les classes de stockage avec leurs valeurs d'API correspondantes :

- Stockage à redondance réduite — `REDUCED_REDUNDANCY`
- S3 Express One Zone : `EXPRESS_ONEZONE`
- S3 Glacier Deep Archive : `DEEP_ARCHIVE`
- S3 Glacier Flexible Retrieval : `GLACIER`
- S3 Glacier Instant Retrieval : `GLACIER_IR`
- S3 Intelligent-Tiering : `INTELLIGENT_TIERING`
- S3 One Zone-IA : `ONEZONE_IA`
- S3 Standard : `STANDARD`
- S3 Standard-IA : `STANDARD_IA`

Définition de la classe de stockage d'un nouvel objet

Pour définir la classe de stockage lors du chargement d'un objet, vous pouvez utiliser les méthodes suivantes.

Utilisation de la console S3

Pour définir la classe de stockage lors du chargement d'un nouvel objet dans la console :

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse suivante : https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment dans lequel vous souhaitez télécharger vos dossiers ou fichiers.
4. Choisissez Charger.

5. Dans la fenêtre Charger, choisissez Propriétés.
6. Sous Classe de stockage, choisissez une classe de stockage pour les fichiers que vous chargez.
7. (Facultatif) Configurez toutes les propriétés supplémentaires pour les fichiers que vous chargez. Pour plus d'informations, consultez Chargement d'objets.
8. Dans la fenêtre Charger, procédez de l'une des manières suivantes :
   - Faites glisser les fichiers et les dossiers dans la fenêtre Charger.
   - Choisissez Ajouter un fichier ou Ajouter un dossier, puis choisissez les fichiers ou les dossiers à charger et Ouvrir.
9. Au bas de la page, choisissez Charger.

Utilisation de l'API REST

Vous pouvez spécifier la classe de stockage d'un objet lorsque vous le créez à l'aide des opérations d'API `PutObject`, `POST Object` ou `CreateMultipartUpload`, et ajoutez l'en-tête de demande `x-amz-storage-class`. Si vous n'ajoutez pas cet en-tête, Amazon S3 utilise la classe de stockage S3 Standard (`STANDARD`) par défaut.

Cet exemple de demande utilise la commande `PutObject` pour définir la classe de stockage d'un nouvel objet sur S3 Intelligent-Tiering :

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

En utilisant le AWS CLI

Cet exemple utilise la `put-object` commande pour télécharger le fichier *`my_images.tar.bz2`* vers *`amzn-s3-demo-bucket1`* dans la classe *`GLACIER`* de stockage :

```
aws s3api put-object --bucket amzn-s3-demo-bucket1 --key dir-1/my_images.tar.bz2 --
storage-class GLACIER --body my_images.tar.bz2
```

Si la taille de l'objet est supérieure à 5 Go, utilisez la commande suivante pour définir la classe de stockage :

```
aws s3 cp large_test_file s3://amzn-s3-demo-bucket1 --storage-class GLACIER
```

Modification de la classe de stockage d'un objet existant

Pour définir la classe de stockage lors du chargement d'un objet, vous pouvez utiliser les méthodes suivantes.

Utilisation de la console S3

Vous pouvez changer la classe de stockage d'un objet à l'aide de la console Amazon S3 si la taille de l'objet est inférieure à 5 Go. Pour une taille supérieure, nous vous recommandons d'ajouter une configuration de cycle de vie S3 pour changer la classe de stockage de l'objet.

Pour modifier la classe de stockage d'un objet dans la console :

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant les objets que vous souhaitez modifier.
4. Cochez la case située à gauche du nom des objets que vous souhaitez modifier.
5. Dans le menu Actions, choisissez Modifier la classe de stockage à partir de la liste d'options qui s'affiche.
6. Sélectionnez l'une des classes de stockage disponibles pour votre objet.
7. Sous Paramètres de copie supplémentaires, choisissez Copie des paramètres source, Aucune spécification de paramètres ou Spécification des paramètres. L'option par défaut est Copie des paramètres source. Si vous souhaitez uniquement copier l'objet sans les attributs des paramètres source, choisissez Aucune spécification de paramètres. Choisissez Spécifier les

paramètres pour définir les paramètres de classe de stockage ACLs, les balises d'objet, les métadonnées, le chiffrement côté serveur et les sommes de contrôle supplémentaires.

8. En bas à droite, choisissez Enregistrer les modifications. Amazon S3 enregistre les modifications apportées.

Utilisation de l'API REST

Pour modifier la classe de stockage d'un objet existant, utilisez les méthodes suivantes.

Cet exemple de demande utilise la `PutObject` commande pour définir la classe de stockage d'un objet existant sur S3 Intelligent-Tiering :

```
PUT /my-image.jpg HTTP/1.1
Host: amzn-s3-demo-bucket1.s3.Region.amazonaws.com
Date: Wed, 12 Oct 2009 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

En utilisant le AWS CLI

Cet exemple utilise la `cp` commande pour modifier la classe de stockage d'un objet existant de sa classe de stockage actuelle en classe de *DEEP_ARCHIVE* stockage :

```
aws s3 cp object_S3_URI object_S3_URI --storage-class DEEP_ARCHIVE
```

Restriction des autorisations de stratégie d'accès à une classe de stockage spécifique

Lorsque vous accordez des autorisations de stratégie d'accès pour les opérations Amazon S3, vous pouvez utiliser la clé de condition `s3:x-amz-storage-class` pour restreindre la classe de stockage à utiliser lors du stockage des objets chargés. Par exemple, lorsque vous accordez l'autorisation `s3:PutObject`, vous pouvez restreindre les chargements d'objets à une classe de stockage spécifique. Pour un exemple de politique, consultez Exemple : Restreindre les chargements aux objets avec une classe de stockage spécifique.

Pour plus d'informations sur l'utilisation des conditions dans les politiques et une liste complète des clés de condition Amazon S3, consultez les rubriques suivantes :

- Actions, ressources et clés de condition pour Amazon S3 dans la Référence de l'autorisation de service

  Pour plus d'informations sur les autorisations relatives aux opérations d'API S3 par type de ressource S3, consultez Autorisations requises pour les opérations d'API Amazon S3.
- Exemples de politiques de compartiment utilisant des clés de condition

Analyses Amazon S3 - Analyse de classe de stockage

Grâce à l'analyse de classe de stockage Analyses Amazon S3, vous pouvez analyser des modèles d'accès au stockage pour décider à quel moment transférer les données appropriées vers la classe de stockage qui convient. Cette nouvelle fonction Analyses Amazon S3 observe les modèles d'accès aux données pour vous aider à déterminer le moment où passer du stockage STANDARD moins fréquemment utilisé à la classe de stockage STANDARD_IA (« IA » correspondant à « infrequent access », soit accès peu fréquents). Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

Une fois que l'analyse de classe de stockage a observé les modèles d'accès peu fréquents d'un ensemble filtré de données sur une période donnée, vous pouvez utiliser les résultats d'analyse pour vous aider à améliorer vos configurations de cycle de vie. Vous pouvez configurer l'analyse de classe de stockage pour analyser tous les objets d'un compartiment. Ou, vous pouvez configurer des filtres pour regrouper des objets pour l'analyse par préfixe commun (c'est-à-dire des objets qui ont des noms qui commencent par une chaîne courante), par balises d'objets, ou par préfixe et balises. Vous trouverez très probablement qu'un filtrage par groupes d'objets est le meilleur moyen de tirer parti de l'analyse de classe de stockage.

> **Important**
>
> L'analyse de classe de stockage fournit uniquement des recommandations pour les classes standard à standard – Accès peu fréquent.

Vous pouvez avoir plusieurs filtres d'analyse de classe de stockage par compartiment, jusqu'à 1 000, et vous recevrez une analyse distincte pour chaque filtre. Plusieurs configurations de filtres vous

permettent d'analyser des groupes spécifiques d'objets pour améliorer vos configurations de cycle de vie qui transfèrent des objets vers STANDARD_IA.

L'analyse de classe de stockage affiche des visualisations de l'utilisation du stockage dans la console Amazon S3 qui sont mises à jour quotidiennement. Vous pouvez également exporter ces données d'utilisation quotidienne vers un compartiment S3 et les afficher dans une application de feuille de calcul, ou avec des outils de veille décisionnelle, comme QuickSight.

Il y a des coûts associés à l'analyse de la classe de stockage. Pour plus d'informations sur les tarifs, consultez Gestion et informations sur la tarification d'Amazon S3.

Rubriques

- Comment configurer une analyse de classe de stockage ?
- Comment utiliser l'analyse de classe de stockage ?
- Comment exporter des données d'analyse de classe de stockage ?
- Configuration d'une analyse de classe de stockage

Comment configurer une analyse de classe de stockage ?

Vous configurez l'analyse de classe de stockage en configurant les données d'objet que vous voulez analyser. Vous pouvez configurer l'analyse de classe de stockage pour effectuer les opérations suivantes :

- Analyser l'ensemble des contenus d'un compartiment.

  Vous recevrez une analyse pour tous les objets du compartiment.
- Analyser les objets regroupés par préfixe et balises.

  Vous pouvez configurer des filtres qui regroupent des objets pour l'analyse par préfixe, par balises d'objets ou par une combinaison de préfixe et de balises. Vous recevez une analyse distincte pour chaque filtre que vous configurez. Vous pouvez avoir plusieurs configurations de filtres par compartiment, jusqu'à 1 000.
- Exporter les données d'analyse.

  Lorsque vous configurez l'analyse de classe de stockage pour un compartiment ou un filtre, vous pouvez choisir que les données d'analyse exportées soient exportées dans un fichier chaque jour. L'analyse du jour est ajoutée au fichier pour former un journal d'analyse historique du filtre

configuré. Le fichier est mis à jour quotidiennement au lieu de destination de votre choix. Lors de la sélection des données à exporter, vous spécifiez un compartiment de destination et un préfixe de destination facultatif où le fichier est écrit.

Vous pouvez utiliser la console Amazon S3, l'API REST ou le AWS CLI or AWS SDKs pour configurer l'analyse des classes de stockage.

- Pour en savoir plus sur la configuration de l'analyse de classe de stockage dans la console Amazon S3, consultez Configuration d'une analyse de classe de stockage.
- Pour utiliser l'API Amazon S3, utilisez l'PutBucketAnalyticsConfigurationAPI REST, ou l'équivalent, depuis le AWS CLI ou AWS SDKs.

Comment utiliser l'analyse de classe de stockage ?

Vous utilisez l'analyse de classe de stockage pour observer vos modèles d'accès aux données dans le temps en vue de collecter des informations vous permettant d'améliorer la gestion du cycle de vie de votre stockage STANDARD_IA. Une fois qu'un filtre est configuré, vous commencez à voir l'analyse des données basée sur le filtre dans la console Amazon S3 dans les 24 à 48 heures. Toutefois, l'analyse de classe de stockage observe les modèles d'accès d'un ensemble filtré de données pendant 30 jours ou plus afin d'obtenir des informations pour l'analyse avant de fournir un résultat. L'analyse se poursuit après le résultat initial et met à jour le résultat à mesure que les modèles d'accès changent

Lorsque vous configurez un filtre pour la première fois, la console Simple Storage Service (Amazon S3) peut prendre du temps pour analyser vos données.

L'analyse de classe de stockage observe les modèles d'accès d'un ensemble filtré de données d'objet pendant 30 jours ou plus pour collecter suffisamment d'informations pour l'analyse. Une fois que l'analyse de classe de stockage a rassemblé suffisamment d'informations, un message indiquant que l'analyse a été complétée s'affiche dans la console Amazon S3.

Lors de l'analyse des objets faisant l'objet d'accès peu fréquents, la classe de stockage examine le jeu filtré d'objets regroupés en fonction de l'âge comme ils ont été téléchargés vers Amazon S3. L'analyse de classe de stockage détermine si la tranche d'âge fait l'objet d'accès peu fréquents en regardant les facteurs suivants de l'ensemble filtré de données :

- Objets de la classe de stockage STANDARD de plus de 128 Ko.
- Stockage total moyen à disposition par tranche d'âge.

- Nombre moyen d'octets transférés (et non la fréquence) par tranche d'âge.
- Les données d'exportation d'analyse incluent uniquement les demandes avec des données pertinentes pour l'analyse de classe de stockage. Cela peut entraîner des différences dans le nombre de demandes, et dans le total des octets de chargement et de demande par rapport à ce qui est affiché dans les métriques de stockage ou suivi dans vos propres système internes.
- Les demandes GET et PUT en échec ne sont pas comptabilisées pour l'analyse. Cependant, vous voyez les demandes en échec dans les métriques de stockage.

Quelle quantité de données a été extraite du stockage ?

La console Amazon S3 affiche la quantité de stockage de l'ensemble de données filtré qui a été récupérée pour la période d'observation.

Quel pourcentage de données a été extrait du stockage ?

La console Amazon S3 affiche également le pourcentage de stockage de l'ensemble de données filtré qui a été récupéré pour la période d'observation.

Comme indiqué précédemment dans cette rubrique, lorsque vous exécutez l'analyse pour les objets faisant l'objet d'accès peu fréquents, l'analyse de classe de stockage examine le jeu filtré d'objets regroupés en fonction de l'âge comme ils ont été chargés dans Amazon S3. L'analyse de classe de stockage utilise les tranches d'âge d'objets prédéfinies suivantes :

- Objets Amazon S3 ayant moins de 15 jours
- Objets Amazon S3 ayant entre 15 et 29 jours
- Objets Amazon S3 ayant entre 30 et 44 jours
- Objets Amazon S3 ayant entre 45 et 59 jours
- Objets Amazon S3 ayant entre 60 et 74 jours
- Objets Amazon S3 ayant entre 75 et 89 jours
- Objets Amazon S3 ayant entre 90 et 119 jours
- Objets Amazon S3 ayant entre 120 et 149 jours
- Objets Amazon S3 ayant entre 150 et 179 jours
- Objets Amazon S3 ayant entre 180 et 364 jours
- Objets Amazon S3 ayant entre 365 et 729 jours
- Objets Amazon S3 ayant 730 jours et plus

Généralement, il faut environ 30 jours d'observation des modes d'accès pour collecter suffisamment d'informations pour un résultat d'analyse. Cette opération peut durer plus de 30 jours, selon le modèle d'accès unique de vos données. Toutefois, une fois qu'un filtre est configuré, vous commencez à voir l'analyse des données basée sur le filtre dans la console Amazon S3 dans les 24 à 48 heures. Vous pouvez voir quotidiennement l'analyse de l'accès aux objets réparti par tranche d'âge d'objets dans la console Amazon S3.

Quelle quantité de données du stockage fait l'objet d'accès peu fréquents ?

La console Amazon S3 affiche les modèles d'accès regroupés par groupes d'âge d'objets prédéfinis. Le texte Frequently accessed (Accès fréquent) ou Infrequently accessed (Accès peu fréquent) est conçu comme une aide visuelle pour vous aider dans le processus de création du cycle de vie.

Comment exporter des données d'analyse de classe de stockage ?

Vous pouvez choisir que le rapport d'analyse de classe de stockage soit au format de fichier plat CSV (valeurs séparées par une virgule). Les rapports sont mis à jour quotidiennement et sont basés sur les filtres de tranche d'âge d'objet que vous configurez. Lorsque vous utilisez la console Amazon S3, vous pouvez choisir l'option d'exportation des rapports quand vous créez un filtre. Lors de la sélection des données à exporter, vous spécifiez un compartiment de destination et un préfixe de destination facultatif où le fichier est écrit. Vous pouvez exporter les données vers un compartiment de destination d'un autre compte. Le compartiment de destination doit se trouver dans la même Région que le compartiment que vous configurez pour être analysé.

Vous devez créer une politique de compartiment sur le compartiment de destination afin d'accorder des autorisations à Amazon S3 afin de vérifier à qui Compte AWS appartient le compartiment et d'écrire des objets dans le compartiment à l'emplacement défini. Pour un exemple de politique, consultez Accorder des autorisations pour l'inventaire S3 et les analyses S3..

Une fois les rapports d'analyse de classe de stockage configurés, vous commencez à obtenir le rapport exporté quotidiennement au bout de 24 heures. Passé ce délai, Amazon S3 continue de surveiller et de fournir des exportations quotidiennes.

Vous pouvez ouvrir le fichier CSV dans un tableur ou l'importer dans d'autres applications comme Amazon QuickSight. Pour plus d'informations sur l'utilisation des fichiers Amazon S3 avec Amazon QuickSight, consultez la section Création d'un ensemble de données à l'aide de fichiers Amazon S3 dans le guide de QuickSight l'utilisateur Amazon.

Les données du fichier exporté sont triées par date dans la tranche d'âge d'objets, comme illustré dans les exemples suivants. Si la classe de stockage est STANDARD, la ligne

contient également les données des colonnes `ObjectAgeForSIATransition` et `RecommendedObjectAgeForSIATransition`.

Date	ConfigId	Filter	StorageClass	ObjectAge	ObjectCount	DataUploaded_MB	Storage_MB	DataRetrieved_MB	GetRequestCount	CumulativeAccessRatio	ObjectAgeForSIATransition	RecommendedObjectAgeForSIATransition
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/2/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	000-014			0.4313			0		
9/5/2021	SalesMaterial	SalesMaterial	STANDARD	000-014						0.04096734		

À la fin du rapport, la tranche d'âge d'objets est nommée ALL. Les lignes ALL contiennent les totaux cumulés de toutes les tranche d'âge pour cette journée, y compris pour les objets inférieurs à 128 Ko.

8/24/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014	
9/3/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.02426125	015-029	
8/28/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.03545875	015-029	
8/17/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014	
8/25/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014	
9/6/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.0209529	015-029	
9/4/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.02304819	015-029	
8/22/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014	
8/21/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014	
8/30/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0.03073092	015-029	
8/20/2021	SalesMaterial	SalesMaterial	STANDARD	ALL	3		0.4599			0	000-014	

La section suivante décrit les colonnes utilisées dans le rapport.

Disposition du fichier exporté

Le tableau suivant décrit la mise en page du fichier d'exportation d'analyse de la classe de stockage Amazon S3.

Configuration d'une analyse de classe de stockage

Grâce à l'outil d'analyse de classe de stockage Amazon S3, vous pouvez analyser des modèles d'accès au stockage pour décider à quel moment transférer les données appropriées vers la classe de stockage qui convient. L'analyse de classe de stockage observe les modèles d'accès aux données pour vous aider à déterminer quand il faut passer du mode STANDARD au mode STANDARD_IA (« IA » correspondant à « infrequent access », soit accès peu fréquent). Pour plus d'informations sur STANDARD_IA, consultez la FAQ Amazon S3 et Bien comprendre et gérer les classes de stockage Amazon S3.

Vous configurez l'analyse de classe de stockage en configurant les données d'objet que vous voulez analyser. Vous pouvez configurer l'analyse de classe de stockage pour effectuer les opérations suivantes :

- Analyser l'ensemble des contenus d'un compartiment.

  Vous recevrez une analyse pour tous les objets du compartiment.
- Analyser les objets regroupés par préfixe et balises.

Vous pouvez configurer des filtres qui regroupent des objets pour l'analyse par préfixe, par balises d'objets ou par une combinaison de préfixe et de balises. Vous recevez une analyse distincte pour chaque filtre que vous configurez. Vous pouvez avoir plusieurs configurations de filtres par compartiment, jusqu'à 1 000.

- Exporter les données d'analyse.

  Lorsque vous configurez l'analyse de classe de stockage pour un compartiment ou un filtre, vous pouvez choisir que les données d'analyse exportées soient exportées dans un fichier chaque jour. L'analyse du jour est ajoutée au fichier pour former un journal d'analyse historique du filtre configuré. Le fichier est mis à jour quotidiennement au lieu de destination de votre choix. Lors de la sélection des données à exporter, vous spécifiez un compartiment de destination et un préfixe de destination facultatif où le fichier est écrit.

Vous pouvez utiliser la console Amazon S3, l'API REST ou le AWS CLI or AWS SDKs pour configurer l'analyse des classes de stockage.

> **Important**
>
> L'analyse de classe de stockage ne fournit pas de recommandations pour les transitions vers les classes de stockage One Zone-IA ou S3 Glacier Flexible Retrieval.
> Si vous souhaitez configurer l'analyse des classes de stockage pour exporter vos résultats sous forme de fichier .csv et que le compartiment de destination utilise le chiffrement de compartiment par défaut avec un AWS KMS key, vous devez mettre à jour la politique AWS KMS clé afin d'accorder à Amazon S3 l'autorisation de chiffrer le fichier .csv. Pour obtenir des instructions, consultez Octroi à Amazon S3 d'utiliser votre clé gérée par le client pour le chiffrement.

Pour plus d'informations sur l'analytique, consultez Analyses Amazon S3 - Analyse de classe de stockage.

Utilisation de la console S3

Pour configurer une analyse de classe de stockage

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation de gauche, choisissez General Purpose buckets ou Directory buckets.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez configurer l'analyse des classes de stockage.
4. Sélectionnez l'onglet Métriques.
5. Sous Analyse des classes de stockage, choisissez Créer une configuration d'analyse.
6. Attribuez un nom au filtre. Pour analyser le compartiment entier, n'indiquez rien dans le champ Préfixe.
7. Dans le champ Préfixe, saisissez du texte pour le préfixe des objets que vous souhaitez analyser.
8. Pour ajouter une balise, choisissez Ajouter une balise. Saisissez une clé et une valeur pour la balise. Vous pouvez entrer un préfixe et plusieurs balises.
9. Vous pouvez également choisir Activer sous Exporter vers CSV pour exporter des rapports d'analyse au format de fichier plat de valeurs séparées par une virgule (.csv). Choisissez un compartiment de destination dans lequel le fichier peut être stocké. Vous pouvez saisir un préfixe pour le compartiment de destination. Le compartiment de destination doit se trouver dans le même compartiment Région AWS que celui pour lequel vous configurez l'analyse. Le compartiment de destination peut se trouver dans un autre Compte AWS.

   Si le compartiment de destination du fichier .csv utilise le chiffrement de compartiment par défaut avec une clé KMS, vous devez mettre à jour la politique relative aux AWS KMS clés pour autoriser Amazon S3 à chiffrer le fichier .csv. Pour obtenir des instructions, consultez Octroi à Amazon S3 d'utiliser votre clé gérée par le client pour le chiffrement.
10. Choisissez Créer une configuration.

Amazon S3 crée une politique de compartiment sur le compartiment de destination qui accorde à Amazon S3 une autorisation en écriture. Cela l'autorise à écrire les données d'exportation dans le compartiment.

Si une erreur se produit lorsque vous tentez de créer la politique de compartiment, des instructions s'affichent pour vous indiquer comment la résoudre. Par exemple, si vous avez choisi un compartiment de destination dans un autre Compte AWS et ne disposez pas des autorisations nécessaires pour lire et écrire dans la politique de compartiment, le message suivant s'affiche. Vous devez demander au propriétaire du compartiment de destination d'ajouter la politique de compartiment affichée au compartiment de destination. Si la stratégie n'est pas ajoutée au

compartiment de destination, vous ne recevez pas les données d'exportation, car Amazon S3 n'est pas autorisé à écrire dans le compartiment de destination. Si le compartiment source est détenu par un compte autre que celui de l'utilisateur actuel, l'ID de compte correct du compartiment source doit être remplacé dans la stratégie.

Pour plus d'informations sur les données exportées et le fonctionnement du filtre, consultez Analyses Amazon S3 - Analyse de classe de stockage.

Utilisation de l'API REST

Pour configurer l'analyse des classes de stockage à l'aide de l'API REST, utilisez le PutBucketAnalyticsConfiguration. Vous pouvez également utiliser l'opération équivalente avec le AWS CLI ou AWS SDKs.

Vous pouvez utiliser le REST suivant APIs pour travailler avec l'analyse des classes de stockage :

- DELETE Bucket Analytics configuration
- GET Bucket Analytics configuration
- List Bucket Analytics Configuration

Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering

La classe de stockage S3 Intelligent-Tiering est conçue pour optimiser les coûts de stockage en déplaçant automatiquement les données vers le niveau d'accès de stockage le plus rentable lorsque les modèles d'accès changent, sans incidence sur les performances ni sur les frais d'exploitation. Moyennant des frais mensuels minimes de surveillance et d'automatisation des objets, S3 Intelligent-Tiering surveille les modèles d'accès et déplace automatiquement les objets qui n'ont pas été consultés vers des niveaux d'accès moins coûteux.

S3 Intelligent-Tiering permet de réduire automatiquement les coûts de stockage grâce à trois niveaux d'accès à faible latence et à haut débit. Pour les données accessibles de manière asynchrone, vous pouvez choisir d'activer les capacités d'archivage automatique dans la classe de stockage S3 Intelligent-Tiering. L'utilisation de S3 Intelligent-Tiering n'entraîne aucuns frais de récupération. Si un objet du niveau d'accès Peu fréquent ou Archive Instant est consulté ultérieurement, il est automatiquement replacé dans le niveau d'accès Fréquent. Aucuns frais supplémentaires ne s'appliquent lorsque des objets sont déplacés entre des niveaux d'accès de la classe de stockage S3 Intelligent-Tiering.

S3 Intelligent-Tiering est la classe de stockage recommandée pour les données avec des modèles d'accès inconnus, changeants ou imprévisibles, indépendamment de la taille de l'objet ou de la période de rétention, telles que les lacs de données, l'analytique des données et les nouvelles applications.

La classe de stockage S3 Intelligent-Tiering prend en charge toutes les fonctions Amazon S3, y compris les suivantes :

- S3 Inventory, pour vérifier le niveau d'accès des objets
- S3 Replication, pour répliquer des données vers n'importe quel Région AWS
- S3 Storage Lens, pour afficher les métriques d'utilisation et d'activité du stockage
- Chiffrement côté serveur, pour protéger les données objet
- Verrouillage des objets S3, pour empêcher la suppression accidentelle de données
- AWS PrivateLink, pour accéder à Amazon S3 via un point de terminaison privé dans un cloud privé virtuel (VPC)

Pour en savoir sur l'utilisation de S3 Intelligent-Tiering, consultez les sections suivantes :

Rubriques

- Fonctionnement de S3 Intelligent-Tiering
- Utiliser S3 Intelligent-Tiering
- Gestion de S3 Intelligent-Tiering

Fonctionnement de S3 Intelligent-Tiering

La classe de stockage Amazon S3 Intelligent-Tiering stocke automatiquement les objets dans trois niveaux d'accès. Un niveau est optimisé pour les accès fréquents, un niveau à coût réduit est optimisé pour les accès peu fréquents, et un autre niveau au coût très réduit est optimisé pour les données rarement accessibles. Pour un faible coût mensuel de surveillance et d'automatisation des objets, S3 Intelligent-Tiering surveille les modèles d'accès et déplace automatiquement les objets vers le niveau d'accès Peu fréquent lorsque ceux-ci n'ont pas été consultés pendant 30 jours consécutifs. Après 90 jours sans accès, les objets sont déplacés vers le niveau d'accès Archive Instant sans impact sur les performances ni sur les frais d'exploitation.

Pour obtenir le coût de stockage le plus bas sur des données auxquelles on peut accéder en quelques minutes ou quelques heures, activez les capacités d'archivage pour ajouter deux niveaux

d'accès supplémentaires. Vous pouvez répartir les objets sur le niveau d'accès Archive, le niveau d'accès Deep Archive, ou les deux. Avec l'accès Archive, S3 Intelligent-Tiering déplace les objets qui n'ont pas été consultés pendant un minimum de 90 jours consécutifs vers le niveau d'accès Archive. Avec l'accès Deep Archive, S3 Intelligent-Tiering déplace les objets vers le niveau d'accès Deep Archive après un minimum de 180 jours consécutifs sans accès. Pour les deux niveaux, vous pouvez configurer le nombre de jours sans accès en fonction de vos besoins.

Les actions suivantes constituent un accès qui empêche de classer vos objets dans le niveau d'accès Archive ou le niveau d'accès Deep Archive :

- Télécharger ou copier un objet archivé via la console Amazon S3.
- Invoquer CopyObject, UploadPartCopy, ou en répliquant des objets avec S3 Batch Replication. Dans ces cas, les objets source des opérations de copie ou de réplication sont hiérarchisés.
- Invoquer GetObject, PutObject, RestoreObject, CompleteMultipartUpload, ListParts, ou SelectObjectContent.

Par exemple, si vous accédez à vos objets via `SelectObjectContent` avant le nombre de jours sans accès que vous avez spécifié (180 jours, par exemple), cette action réinitialise le chronomètre. Vos objets ne sont pas déplacés vers le niveau d'accès Archive ni vers le niveau d'accès Deep Archive tant que la dernière demande `SelectObjectContent` n'a pas atteint le nombre de jours spécifiés.

Si un objet du niveau d'accès Peu fréquent ou Archive Instant est consulté ultérieurement, il est automatiquement replacé dans le niveau d'accès Fréquent.

Les actions suivantes constituent un accès qui renvoie automatiquement des objets du niveau d'accès Peu fréquent ou Archive Instant vers le niveau d'accès Fréquent :

- Télécharger ou copier un objet archivé via la console Amazon S3.
- Invoquer CopyObject, UploadPartCopy, ou en répliquant des objets avec Batch Replication. Dans ces cas, les objets source des opérations de copie ou de réplication sont hiérarchisés.
- Invoquer GetObject, PutObject, RestoreObject, CompleteMultipartUpload, ou ListParts.

Les autres actions ne constituent pas un accès qui renvoie automatiquement des objets du niveau d'accès Peu fréquent ou Archive Instant vers le niveau d'accès Fréquent. Voici un exemple, et non une liste définitive, de telles actions :

- Invoquer HeadObject, GetObjectTagging, PutObjectTagging, ListObjects, ListObjectsV2, ou ListObjectVersions.
- Invoquer SelectObjectContentne constitue pas un accès hiérarchisant les objets jusqu'à un niveau d'accès fréquent. De plus, elle n'empêche pas de hiérarchiser les objets du niveau d'accès fréquent au niveau d'accès peu fréquent, puis jusqu'au niveau Archive Instant Access.

Vous pouvez utiliser S3 Intelligent-Tiering comme classe de stockage par défaut pour les données nouvellement créées en spécifiant `INTELLIGENT-TIERING` dans l'en-tête de demande `x-amz-storage-class` lorsque vous appelez les opérations `PutObject`, `CopyObject` ou `CreateMultipartUpload`. S3 Intelligent-Tiering est conçue pour une disponibilité de 99,9 % et une durabilité de 99,9999999 %.

> **Note**
>
> Si la taille d'un objet est inférieure à 128 Ko, il n'est pas contrôlé et n'est pas admissible à la hiérarchisation automatique. Les objets plus petits sont toujours stockés dans le niveau Accès fréquent.

Niveaux d'accès S3 Intelligent-Tiering.

La section suivante explique les différents niveaux d'accès automatiques et facultatifs. Lorsque des objets se déplacent entre les niveaux d'accès, la classe de stockage reste la même (S3 Intelligent-Tiering).

Niveau Accès fréquent (automatique)

C'est le niveau d'accès par défaut dans lequel tout objet créé ou migré dans S3 Intelligent-Tiering commence son cycle de vie. Un objet reste dans ce niveau tant qu'il est accessible. Le niveau d'accès fréquent offre une faible latence et des performances de débit élevées.

Niveau d'accès peu fréquent (automatique)

Si vous n'accédez pas à un objet pendant 30 jours consécutifs, il passera au niveau Accès peu fréquent. Le niveau d'accès peu fréquent offre une faible latence et des performances de débit élevées.

Niveau d'accès Archive Instant (automatique)

Si vous n'accédez pas à un objet pendant 90 jours consécutifs, il passera au niveau d'accès Archive Instant. Le niveau Archive Instant Access offre une faible latence et des performances de débit élevées.

Niveau d'accès Archive (facultatif)

S3 Intelligent-Tiering vous offre la possibilité d'activer le niveau d'accès Archive pour les données accessibles de manière asynchrone. Une fois activé, le niveau d'accès Archive archive automatiquement les objets qui n'ont pas été consultés pendant un minimum de 90 jours consécutifs. Vous pouvez prolonger le délai de dernier accès pour l'archivage jusqu'à un maximum de 730 jours. Le niveau d'accès Archive offre les mêmes performances que la classe de stockage S3 Glacier Flexible Retrieval.

Les temps de récupération standard pour ce niveau d'accès peuvent varier de 3 à 5 heures. Si vous lancez votre demande de restauration à l'aide d'opérations par lot S3, votre restauration démarre en quelques minutes. Pour plus d'informations sur les options et les durées de récupération, consultez the section called "Restauration des objets à partir des niveaux d'accès Archive et Deep Archive de S3 Intelligent-Tiering".

> **Note**
>
> N'activez le niveau d'accès Archive que pendant 90 jours si vous souhaitez contourner le niveau d'accès Archive Instant. Le niveau Archive Access permet de réduire légèrement les coûts de stockage, avec des délais de minute-to-hour récupération. Le niveau d'accès Archive Instant offre un accès de l'ordre de la milliseconde et des performances à haut débit.

Niveau d'accès Deep Archive (facultatif)

S3 Intelligent-Tiering vous offre la possibilité d'activer le niveau d'accès Deep Archive pour les données accessibles de manière asynchrone. Une fois activé, le niveau d'accès Deep Archive archive automatiquement les objets qui n'ont pas été consultés pendant un minimum de 180 jours consécutifs. Vous pouvez prolonger le délai de dernier accès pour l'archivage jusqu'à un maximum de 730 jours. Le niveau d'accès Deep Archive offre les mêmes performances que la classe de stockage S3 Glacier Deep Archive.

La récupération standard des objets dans ce niveau d'accès a lieu dans les 12 heures. Si vous lancez votre demande de restauration à l'aide d'opérations par lot S3, votre restauration démarre dans les 9 heures. Pour plus d'informations sur les options et les durées de récupération, consultez the section called "Restauration des objets à partir des niveaux d'accès Archive et Deep Archive de S3 Intelligent-Tiering".

> **Note**
>
> Activez les niveaux d'accès Archive et Deep Archive uniquement si vos objets sont accessibles de manière asynchrone par votre application. Si l'objet que vous récupérez est stocké au niveau d'accès Archive ou Deep Archive, vous devez d'abord restaurer l'objet à l'aide de l'opération `RestoreObject`.

Utiliser S3 Intelligent-Tiering

Vous pouvez utiliser la classe de stockage S3 Intelligent-Tiering afin d'optimiser automatiquement les coûts de stockage. S3 Intelligent-Tiering permet de réaliser automatiquement des économies en déplaçant les données à un niveau d'objet granulaire entre les niveaux d'accès lorsque les modèles d'accès changent. Pour les données accessibles de manière asynchrone, vous pouvez choisir d'activer l'archivage automatique au sein de la classe de stockage S3 Intelligent-Tiering à l'aide de l'API, AWS Management Console ou AWS CLI Amazon S3.

Déplacement des données vers S3 Intelligent-Tiering

Il existe deux façons de déplacer des données vers S3 Intelligent-Tiering. Vous pouvez charger des objets directement dans S3 Intelligent-Tiering depuis la console ou par programmation à l'aide d'une opération PUT. Pour de plus amples informations, veuillez consulter Définition de la classe de stockage d'un objet. Vous pouvez également configurer des configurations du cycle de vie S3 pour transférer des objets depuis S3 Standard ou S3 Standard-Infrequent Access vers S3 Intelligent-Tiering.

Chargement de données vers S3 Intelligent-Tiering à l'aide de Direct PUT

Lorsque vous chargez un objet vers la classe de stockage S3 Intelligent-Tiering à l'aide de l'opération d'API PUT, vous spécifiez S3 Intelligent-Tiering dans l'en-tête de demande `x-amz-storage-class`.

La requête suivante stocke l'image, `my-image.jpg`, dans le `myBucket`compartiment. La requête utilise l'en-tête `x-amz-storage-class` pour demander que l'objet soit stocké à l'aide de la classe de stockage S3 Intelligent-Tiering.

Example

```
PUT /my-image.jpg HTTP/1.1
Host: myBucket.s3.<Region>.amazonaws.com (http://amazonaws.com/)
Date: Wed, 1 Sep 2021 17:50:00 GMT
Authorization: authorization string
Content-Type: image/jpeg
Content-Length: 11434
Expect: 100-continue
x-amz-storage-class: INTELLIGENT_TIERING
```

Transition des données vers S3 Intelligent-Tiering depuis S3 standard ou S3 Standard-Accès peu fréquent à l'aide du cycle de vie S3

Vous pouvez ajouter des règles à une configuration de cycle de vie S3 afin d'indiquer à Amazon S3 d'effectuer la transition des objets d'une classe de stockage vers une autre. Pour plus d'informations sur les transitions prises en charge et les contraintes associées, consultez Transition des objets à l'aide du cycle de vie S3.

Vous pouvez spécifier des configurations de cycle de vie S3 au niveau du compartiment ou du préfixe. Dans cette règle de configuration de cycle de vie S3, le filtre spécifie un préfixe de clé (`documents/`). Par conséquent, la règle s'applique aux objets avec le préfixe du nom de clé `documents/`, comme `documents/doc1.txt` et `documents/doc2.txt`. La règle spécifie une action `Transition` indiquant à Amazon S3 d'effectuer la transition d'objets vers la classe de stockage S3 Intelligent-Tiering 0 jour après leur création. Dans ce cas, les objets sont admissibles à la transition vers S3 Intelligent-Tiering à minuit TUC après leur création.

Example

```
<LifecycleConfiguration>
  <Rule>
    <ID>ExampleRule</ID>
    <Filter>
       <Prefix>documents/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
```

```
      <Days>0</Days>
      <StorageClass>INTELLIGENT_TIERING</StorageClass>
    </Transition>
 </Rule>
</LifecycleConfiguration>
```

Un compartiment activé pour la gestion des versions maintient une version d'objet actuelle et aucune ou plusieurs versions d'objets anciennes. Vous pouvez définir des règles de cycle de vie séparées pour les versions d'objet actuelles et anciennes.

Pour de plus amples informations, veuillez consulter Éléments de la configuration du cycle de vie.

Activation des niveaux d'accès S3 Intelligent-Tiering Archive et Deep Archive

Pour obtenir le coût de stockage le plus bas possible sur les données accessibles en quelques minutes ou quelques heures, vous pouvez activer l'un des niveaux d'accès aux archives ou les deux en créant une configuration au niveau du bucket, du préfixe ou de la balise d'objet à l'aide de l'API AWS Management Console AWS CLI, ou Amazon S3.

Utilisation de la console S3

Activer l'archivage automatique S3 Intelligent-Tiering

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le nom du compartiment que vous souhaitez utiliser.
3. Choisissez Propriétés.
4. Accédez à la section Configuration d'archivage S3 Intelligent-Tiering, puis choisissez Créer une configuration.
5. Dans la section Paramètres de configuration d'archivage, précisez un nom de configuration descriptif pour votre configuration d'archivage S3 Intelligent-Tiering.
6. Sous Choisir une portée de configuration, choisissez une portée de configuration à utiliser. Le cas échéant, vous pouvez limiter la portée de configuration aux objets spécifiés dans un compartiment à l'aide d'un préfixe partagé, d'une balise d'objet ou d'une combinaison des deux.

    a. Pour limiter la portée de la configuration, sélectionnez Limiter la portée de cette configuration à l'aide d'un ou de plusieurs filtres.

    b. Pour limiter la portée de la configuration à l'aide d'un préfixe unique, saisissez le préfixe sous Préfixe.

c. Pour limiter la portée de la configuration à l'aide de balises d'objet, sélectionnez Ajouter une balise, puis saisissez une valeur de clé.

7. Sous État, sélectionnez Activer.
8. Dans la section Paramètres Archive, sélectionnez l'un ou les deux niveaux d'accès Archive à activer.
9. Sélectionnez Create (Créer).

À l'aide du AWS CLI

Vous pouvez utiliser les AWS CLI commandes suivantes pour gérer les configurations S3 Intelligent-Tiering :

- `delete-bucket-intelligent-tiering-configuration`
- `get-bucket-intelligent-tiering-configuration`
- `list-bucket-intelligent-tiering-configurations`
- `put-bucket-intelligent-tiering-configuration`

Pour obtenir des instructions sur la configuration du AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

Lorsque vous utilisez le AWS CLI, vous ne pouvez pas spécifier la configuration sous forme de fichier XML. Vous devez spécifier le format JSON à la place. Voici un exemple de configuration S3 Intelligent-Tiering au format XML et de son équivalent au format JSON que vous pouvez spécifier dans une commande AWS CLI .

L'exemple suivant montre comment placer une configuration S3 Intelligent-Tiering dans le compartiment spécifié.

Example **`put-bucket-intelligent-tiering-configuration`**

JSON

```
{
  "Id": "string",
  "Filter": {
    "Prefix": "string",
    "Tag": {
      "Key": "string",
```

```
      "Value": "string"
    },
    "And": {
      "Prefix": "string",
      "Tags": [
        {
          "Key": "string",
          "Value": "string"
        }
        ...
      ]
    }
  },
  "Status": "Enabled"|"Disabled",
  "Tierings": [
    {
      "Days": integer,
      "AccessTier": "ARCHIVE_ACCESS"|"DEEP_ARCHIVE_ACCESS"
    }
    ...
  ]
}
```

XML

```
PUT /?intelligent-tiering&id=Id HTTP/1.1
Host: Bucket.s3.amazonaws.com
<?xml version="1.0" encoding="UTF-8"?>
<IntelligentTieringConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
   <Id>string</Id>
   <Filter>
      <And>
         <Prefix>string</Prefix>
         <Tag>
            <Key>string</Key>
            <Value>string</Value>
         </Tag>
         ...
      </And>
      <Prefix>string</Prefix>
      <Tag>
         <Key>string</Key>
         <Value>string</Value>
```

```
      </Tag>
   </Filter>
   <Status>string</Status>
   <Tiering>
      <AccessTier>string</AccessTier>
      <Days>integer</Days>
   </Tiering>
   ...
</IntelligentTieringConfiguration>
```

Utilisation de l'opération d'API PUT

Vous pouvez utiliser l'opération `PutBucketIntelligentTieringConfiguration` pour un compartiment spécifié et jusqu'à 1 000 configurations S3 Intelligent-Tiering par compartiment. Vous pouvez définir les objets d'un compartiment qui peuvent bénéficier des niveaux d'accès Archive à l'aide d'un préfixe partagé ou d'une balise d'objet. Utiliser un préfixe partagé ou une balise d'objet permet de faire correspondre des applications métier, des flux de travail ou des organisations internes spécifiques. Vous avez également la possibilité d'activer le niveau d'accès Archive, le niveau d'accès Deep Archive, ou les deux.

Démarrer avec Amazon S3 Intelligent-Tiering

Pour en savoir plus sur l'utilisation de S3 Intelligent-Tiering, consultez Tutorial: Getting started using S3 Intelligent-Tiering (Tutoriel : démarrer avec Amazon S3 Intelligent-Tiering).

Gestion de S3 Intelligent-Tiering

Le classe de stockage S3 Intelligent-Tiering permet de réduire automatiquement les coûts de stockage grâce à trois niveaux d'accès à faible latence et à haut débit. Il offre également des fonctionnalités d'archivage en option vous permettant de bénéficier des coûts de stockage les plus bas dans le cloud pour les données accessibles sur une période allant de quelques minutes à plusieurs heures.

Identification des objets du niveau d'accès S3 Intelligent-Tiering qui sont stockés dans

Pour obtenir la liste de vos objets et de leurs métadonnées correspondantes, y compris de leur niveau d'accès S3 Intelligent-Tiering, vous pouvez utiliser l'inventaire Amazon S3. S3 Inventory fournit des fichiers CSV, ORC ou Parquet des fichiers de sortie qui répertorient vos objets et leurs métadonnées correspondantes. Vous pouvez recevoir ces rapports d'inventaire sur une base

quotidienne ou hebdomadaire pour un compartiment Amazon S3 ou un préfixe partagé. (Le préfixe partagé fait référence aux objets dont les noms commencent par une chaîne commune.)

Affichage de l'état de l'archive d'un objet dans S3 Intelligent-Tiering

Vous pouvez configurer des notifications d'événements S3 afin d'être informé lorsqu'un objet de la classe de stockage S3 Intelligent-Tiering passe au niveau Archive Access ou Deep Archive Access. Pour plus d'informations, consultez Activation des notifications d'événement.

Amazon S3 peut publier des notifications d'événement dans une rubrique Amazon Simple Notification Service (Amazon SNS), une file d'attente Amazon Simple Queue Service (Amazon SQS) ou une fonction AWS Lambda . Pour de plus amples informations, veuillez consulter Notifications d'événements Amazon S3.

Le message suivant est un exemple de message envoyé par Amazon S3 pour publier un événement `s3:IntelligentTiering`. Pour de plus amples informations, veuillez consulter the section called "Structure des messages d'événements".

```
{
   "Records":[
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"IntelligentTiering",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
```

```
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
            }
         },
         "intelligentTieringEventData":{
            "destinationAccessTier": "ARCHIVE_ACCESS"
            }
      }
   ]
}
```

Vous pouvez également utiliser une demande d'objet HEAD pour afficher le statut d'archivage d'un objet. Si un objet est stocké dans la classe de stockage S3 Intelligent-Tiering et se trouve dans l'un des niveaux d'archivage, la réponse de l'objet HEAD affiche le niveau d'archivage actuel. Pour afficher le niveau d'archivage, la demande utilise le x-amz-archive-statusen-tête.

La demande d'objet HEAD suivante renvoie les métadonnées d'un objet (dans ce cas, *my-image.jpg*).

Example

```
HEAD /my-image.jpg HTTP/1.1
Host: bucket.s3.region.amazonaws.com
Date: Wed, 28 Oct 2009 22:32:00 GMT
Authorization: AWS AKIAIOSFODNN7EXAMPLE:02236Q3V0RonhpaBX5sCYVf1bNRuU=
```

Vous pouvez également utiliser des demandes d'objet HEAD pour surveiller le statut d'une demande `restore-object`. Si la restauration des archives est en cours, la réponse de l'HEADobjet inclut x-amz-restoreen-tête.

L'exemple suivant de réponse d'objet HEAD montre un objet archivé à l'aide de S3 Intelligent-Tiering avec une demande de restauration en cours.

Example

```
HTTP/1.1 200 OK
```

```
x-amz-id-2: FSVaTMjrmBp3Izs1NnwBZeu7M19iI8UbxMbi0A8AirHANJBo+hEftBuiESACOMJp
x-amz-request-id: E5CEFCB143EB505A
Date: Fri, 13 Nov 2020 00:28:38 GMT
Last-Modified: Mon, 15 Oct 2012 21:58:07 GMT
ETag: "1accb31fcf202eba0c0f41fa2f09b4d7"
x-amz-storage-class: 'INTELLIGENT_TIERING'
x-amz-archive-status: 'ARCHIVE_ACCESS'
x-amz-restore: 'ongoing-request="true"'
x-amz-restore-request-date: 'Fri, 13 Nov 2020 00:20:00 GMT'
Accept-Ranges: bytes
Content-Type: binary/octet-stream
Content-Length: 300
Server: AmazonS3
```

Restauration des objets à partir des niveaux d'accès Archive et Deep Archive de S3 Intelligent-Tiering

Pour accéder aux objets des niveaux Archive Access et Deep Archive Access de S3 Intelligent-Tiering, vous devez lancer une demande de restauration, puis attendre que l'objet soit placé au niveau d'accès fréquent. Pour plus d'informations sur les objets archivés, consultez the section called "Utilisation des objets archivés".

Lorsque vous restaurez un objet depuis les niveaux d'accès Archive et Deep Archive, l'objet retourne au niveau d'accès Fréquent. Par la suite, si vous n'accédez pas à l'objet dans les 30 jours consécutifs, il sera automatiquement déplacé vers le niveau d'accès Peu fréquent. Ensuite, après un minimum de 90 jours consécutifs sans accès, l'objet passe au niveau Archive Access. Après un minimum de 180 jours consécutifs sans accès, l'objet passe au niveau Deep Archive Access. Pour de plus amples informations, veuillez consulter the section called "Fonctionnement de S3 Intelligent-Tiering".

Vous pouvez restaurer un objet archivé à l'aide de la console Amazon S3, de S3 Batch Operations, de l'API REST Amazon S3 AWS SDKs, du ou du AWS Command Line Interface (AWS CLI). Pour de plus amples informations, veuillez consulter the section called "Utilisation des objets archivés".

Présentation des classes de stockage S3 Glacier pour le stockage de données à long terme

Vous pouvez utiliser les classes de stockage S3 Glacier d'Amazon S3 pour fournir des solutions économiques de stockage de données à long terme qui ne sont pas souvent consultées. Les classes de stockage S3 Glacier sont :

- S3 Glacier Instant Retrieval

- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive

Le choix d'une de ces classes de stockage dépend de la fréquence à laquelle vous accédez à vos données et de la rapidité avec laquelle vous devez les récupérer. Chacune de ces classes de stockage offre une durabilité et une résilience égales à celles de la classe de stockage S3 standard, mais pour des coûts de stockage inférieurs. Pour plus d'informations sur les classes de stockage S3 Glacier, consultez https://aws.amazon.com/s3/storage-classes/glacier/.

Rubriques

- Comparaison des classes de stockage S3 Glacier
- S3 Glacier Instant Retrieval
- S3 Glacier Flexible Retrieval
- S3 Glacier Deep Archive
- Présentation du stockage d'archivage dans S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive
- Différences entre ces classes de stockage et le service S3 Glacier

Comparaison des classes de stockage S3 Glacier

Chaque classe de stockage S3 Glacier présente une durée de stockage minimale pour tous les objets. Si vous supprimez l'objet, le remplacez ou le transférez dans une autre classe de stockage avant la durée minimale, le reste de cette durée vous est facturé.

Certaines classes de stockage S3 Glacier sont de type archivage, ce qui signifie que les objets stockés dans ces classes sont archivés et ne sont pas disponibles pour un accès en temps réel. Pour de plus amples informations, veuillez consulter Présentation du stockage d'archivage dans S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.

Les classes de stockage conçues pour des modèles d'accès moins fréquents avec des temps de récupération plus longs offrent des coûts de stockage inférieurs. Pour en savoir plus sur la tarification, consultez https://aws.amazon.com/s3/pricing/.

Le tableau suivant récapitule les points clés à prendre en compte lors du choix d'une classe de stockage S3 Glacier :

S3 Glacier Instant Retrieval

Nous recommandons d'utiliser S3 Glacier Instant Retrieval pour des données à long terme auxquelles vous souhaitez accéder une fois par trimestre avec un temps de récupération de quelques millisecondes. Cette classe de stockage est idéale pour les cas d'utilisation sensibles aux performances tels que l'hébergement d'images, les applications de partage de fichiers et le stockage de dossiers médicaux qui doivent être accessibles pendant une consultation.

La classe de stockage S3 Glacier Instant Retrieval offre un accès en temps réel à vos objets avec la même latence et les mêmes performances de débit que la classe de stockage S3 Standard – Accès peu fréquent. Comparée à S3 Standard – Accès peu fréquent, la classe S3 Glacier Instant Retrieval présente des coûts de stockage inférieurs mais des coûts d'accès aux données plus élevés.

Une taille d'objet minimale de 128 Ko s'applique aux données stockées dans la classe de stockage S3 Glacier Instant Retrieval. Cette classe de stockage a également une durée de stockage minimum de 90 jours.

S3 Glacier Flexible Retrieval

Nous recommandons d'utiliser S3 Glacier Flexible Retrieval pour des données d'archive auxquelles vous souhaitez accéder une ou deux fois par an et qui ne nécessitent pas un accès immédiat. S3 Glacier Flexible Retrieval offre des temps de récupération flexibles pour vous aider à équilibrer les coûts, avec des temps d'accès allant de quelques minutes à quelques heures, et des récupérations en bloc gratuites. Cette classe de stockage est idéale pour la sauvegarde et la reprise après sinistre.

Les objets stockés dans S3 Glacier Flexible Retrieval sont archivés et ne sont pas disponibles pour un accès en temps réel. Pour de plus amples informations, veuillez consulter Présentation du stockage d'archivage dans S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive. Pour accéder à ces objets, vous devez d'abord lancer une demande de restauration pour créer une copie temporaire de l'objet auquel vous pourrez accéder une fois la demande terminée. Pour plus d'informations, consultez Utilisation des objets archivés. Lorsque vous restaurez un objet, vous pouvez choisir un niveau de récupération adapté à votre cas d'utilisation, avec des coûts moindres pour des délais de restauration plus longs.

Les niveaux de récupération suivants sont disponibles pour S3 Glacier Flexible Retrieval :

- Récupération accélérée : la restauration de l'objet prend généralement entre 1 et 5 minutes. Les récupérations accélérées dépendent de la demande. Pour garantir des délais de restauration fiables et prévisibles, nous vous recommandons d'acheter une capacité de récupération provisionnée. Pour de plus amples informations, veuillez consulter Capacité provisionnée.

- Récupération standard : la restauration de l'objet prend généralement entre 3 et 5 heures, ou entre 1 minute et 5 heures lorsque vous utilisez les opérations par lot S3. Pour de plus amples informations, veuillez consulter Restauration d'objets à l'aide d'opérations par lot.
- Récupération en bloc : la restauration de l'objet prend généralement entre 5 et 12 heures. Les récupérations en bloc sont gratuites.

La durée minimale de stockage des objets dans la classe de stockage S3 Glacier Flexible Retrieval est de 90 jours.

S3 Glacier Flexible Retrieval nécessite 40 Ko de métadonnées supplémentaires pour chaque objet. Cela inclut 32 Ko de métadonnées nécessaires à l'identification et à la récupération des données, facturés au tarif par défaut pour S3 Glacier Flexible Retrieval. 8 Ko supplémentaires de données sont requis pour conserver le nom et les métadonnées définis par l'utilisateur pour les objets archivés, qui sont facturés au tarif S3 Standard.

S3 Glacier Deep Archive

Nous recommandons d'utiliser S3 Glacier Deep Archive pour les données d'archive consultées moins d'une fois par an. Cette classe de stockage est conçue pour conserver les jeux de données pendant plusieurs années afin de répondre à des exigences de conformité. Elle peut également être utilisée pour la sauvegarde ou la reprise après sinistre ou pour des données quelconques rarement consultées dont vous pouvez attendre la récupération jusqu'à 72 heures. S3 Glacier Deep Archive est l'option de stockage la moins chère dans AWS.

Les objets stockés dans S3 Glacier Deep Archive sont archivés et ne sont pas disponibles pour un accès en temps réel. Pour de plus amples informations, veuillez consulter Présentation du stockage d'archivage dans S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive. Pour accéder à ces objets, vous devez d'abord lancer une demande de restauration pour créer une copie temporaire de l'objet auquel vous pourrez accéder une fois la demande terminée. Pour plus d'informations, consultez Utilisation des objets archivés. Lorsque vous restaurez un objet, vous pouvez choisir un niveau de récupération adapté à votre cas d'utilisation, avec des coûts moindres pour des délais de restauration plus longs.

Les niveaux de récupération suivants sont disponibles pour S3 Glacier Deep Archive :

- Récupération standard : restaure généralement l'objet dans les 12 heures ou entre 9 et 12 heures lorsque vous utilisez les opérations par lot S3. Pour de plus amples informations, veuillez consulter Restauration d'objets à l'aide d'opérations par lot.

- Récupération en bloc : restaure généralement l'objet dans les 48 heures pour une fraction du coût du niveau de récupération standard.

La durée minimale de stockage des objets dans la classe de stockage S3 Glacier Deep Archive est de 180 jours.

S3 Glacier Deep Archive nécessite 40 Ko de métadonnées supplémentaires pour chaque objet. Cela inclut 32 Ko de métadonnées nécessaires à l'identification et à la récupération des données, facturés au tarif par défaut pour S3 Glacier Deep Archive. 8 Ko supplémentaires de données sont requis pour conserver le nom et les métadonnées définis par l'utilisateur pour les objets archivés, qui sont facturés au tarif S3 Standard.

Présentation du stockage d'archivage dans S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive

S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive sont des classes de stockage d'archivage. Cela signifie que lorsque vous stockez un objet dans ces classes de stockage, l'objet est archivé et n'est pas accessible directement. Pour accéder à un objet archivé, vous soumettez une demande de restauration, puis vous attendez que le service restaure l'objet. La demande de restauration restaure une copie temporaire de l'objet, qui est supprimée à l'expiration du délai spécifié dans la demande. Pour de plus amples informations, veuillez consulter Utilisation des objets archivés.

La transition d'objets vers la classe de stockage S3 Glacier Deep Archive est unidirectionnelle.

Si vous souhaitez modifier la classe de stockage d'un objet archivé en une autre classe, vous devez utiliser l'opération de restauration pour effectuer d'abord une copie de l'objet. Utilisez ensuite l'opération de copie pour remplacer l'objet en spécifiant S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou Stockage à redondance réduite comme classe de stockage.

> **Note**
>
> L'opération de copie des objets restaurés n'est pas prise en charge dans la console Amazon S3 pour les objets des classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour ce type d'opération de copie, utilisez l'API AWS Command Line Interface (AWS CLI) AWS SDKs, l'API ou l'API REST.

Vous pouvez restaurer des objets archivés dans ces classes de stockage avec un maximum de 1 000 transactions par seconde (TPS) de demandes de restauration d'objets par compte et par Région AWS.

Considérations de coût

Si vous envisagez d'archiver des données rarement accédées pendant plusieurs mois ou années, les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive peuvent réduire vos coûts de stockage. Toutefois, pour vous assurer que la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive vous convient, tenez compte des éléments suivants :

- Frais de la surcharge de stockage : chaque objet archivé nécessite 40 Ko de métadonnées supplémentaires. Cela inclut 32 Ko de métadonnées nécessaires à l'identification et à la récupération des données, facturés au tarif par défaut de la classe de stockage. 8 Ko supplémentaires de données sont requis pour conserver le nom et les métadonnées définis par l'utilisateur pour les objets archivés, qui sont facturés au tarif S3 Standard.

  Si vous archivez de petits objets, tenez compte de ces frais de stockage. Pensez également à regrouper de nombreux petits objets en un plus petit nombre de gros objets afin de réduire les frais généraux.
- Tarification du téléchargement partitionné : les objets dans S3- storage-class-glacier ; et S3 Glacier Deep Archive sont facturés aux tarifs de classe de stockage standard S3 lorsque vous les chargez à l'aide de téléchargements partitionnés. Pour de plus amples informations, veuillez consulter Chargement partitionné et tarification.
- Frais de stockage minimum de 30 jours : S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive sont des solutions d'archivage à long terme. La durée minimale de stockage est de 90 jours pour la classe de stockage S3 Glacier Flexible Retrieval et de 180 jours pour S3 Glacier Deep Archive. La suppression des données archivées dans ces classes de stockage n'entraîne aucun frais si les objets que vous supprimez sont archivés depuis plus longtemps que la durée de stockage minimale. Si vous supprimez ou remplacez un objet archivé avant la durée minimale, Amazon S3 facture le reste de cette durée.
- Frais de récupération de données : lorsque vous restaurez un objet archivé dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, des frais de récupération de données par demande sont facturés. Ces frais varient en fonction du niveau de récupération que vous choisissez lorsque vous lancez une restauration. Pour en savoir plus sur la tarification, consultez Tarification Amazon S3.

- Cycle de vie S3 : lorsque vous restaurez un objet archivé dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, des frais de récupération de données par demande sont facturés. Ces frais varient en fonction du niveau de récupération que vous choisissez lorsque vous lancez une restauration. Pour en savoir plus sur la tarification, consultez Tarification Amazon S3.

Restauration d'objets archivés

Les objets archivés ne sont pas accessibles en temps réel. Vous devez d'abord lancer une demande de restauration puis attendre jusqu'à ce qu'une copie temporaire de l'objet soit disponible pour la durée spécifiée dans la demande. Une fois que vous avez reçu une copie temporaire de l'objet restauré, la classe de stockage de l'objet reste S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. (Une demande d'opération d'API HeadObject ou GetObject renvoie S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive comme classe de stockage.)

> **Note**
>
> Lorsque vous restaurez une archive, vous payez à la fois l'archive (tarif S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive) et une copie que vous avez restaurée temporairement (tarif de stockage S3 standard). Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3.

Vous pouvez restaurer la copie d'un objet par programmation ou à l'aide de la console Amazon S3. Amazon S3 ne traite qu'une seule demande de restauration simultanée par objet. Pour de plus amples informations, veuillez consulter Restauration d'un objet archivé.

Différences entre ces classes de stockage et le service S3 Glacier

Les classes de stockage S3 Glacier font partie du service Amazon S3 et stockent les données sous forme d'objets dans des compartiments S3. Vous pouvez gérer les objets de ces classes de stockage à l'aide de la console S3 ou par programmation à l'aide de la console S3 APIs ou. SDKs Lorsque vous stockez des objets dans les classes de stockage S3 Glacier, vous pouvez utiliser les fonctionnalités S3 telles que le chiffrement avancé, le balisage des objets et les configurations du cycle de vie S3 pour mieux gérer l'accessibilité et le coût des données.

> **Important**
>
> Nous vous recommandons d'utiliser les classes de stockage S3 Glacier au sein du service Amazon S3 pour toutes vos données à long terme.

Le service Amazon S3 Glacier (S3 Glacier) est un service distinct qui stocke les données sous forme d'archives dans des coffres. Ce service ne prend pas en charge les fonctionnalités Amazon S3 et n'assure pas la prise en charge par une console des opérations de chargement et de téléchargement de données. Nous ne vous recommandons pas d'utiliser le service S3 Glacier pour vos données à long terme. Les données stockées dans ce service ne sont pas accessibles à partir du service Amazon S3. Si vous recherchez des informations sur le service S3 Glacier, consultez le Guide du développeur Amazon S3 Glacier. Pour transférer des données du service Amazon S3 Glacier vers une classe de stockage dans Amazon S3, voir Transfert de données d'Amazon S3 Glacier Vaults vers Amazon S3 dans la bibliothèque de AWS solutions.

Utilisation des objets archivés

Pour réduire vos coûts de stockage pour les objets rarement consultés, vous pouvez archiver ces objets. Lorsque vous archivez un objet, il est placé dans un espace de stockage à faible coût, ce qui signifie que vous ne pouvez pas y accéder en temps réel.

Bien que les objets archivés ne soient pas accessibles en temps réel, vous pouvez les restaurer en quelques minutes ou quelques heures, selon la classe de stockage. Vous pouvez restaurer un objet archivé à l'aide de la console Amazon S3, de S3 Batch Operations, de l'API REST AWS SDKs, du et du AWS Command Line Interface (AWS CLI). Pour obtenir des instructions, consultez Restauration d'un objet archivé.

Les objets Amazon S3 figurant dans les classes ou niveaux de stockage suivants sont archivés et ne sont pas accessibles en temps réel :

- Classe de stockage S3 Glacier Flexible Retrieval
- Classe de stockage S3 Glacier Deep Archive
- Niveau Accès aux archives S3 Intelligent-Tiering.
- Niveau d'accès Deep Archive de S3 Intelligent-Tiering

Pour restaurer les objets archivés, vous devez effectuer les opérations suivantes :

- Pour les objets des classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, vous devez d'abord lancer une demande de restauration, puis attendre qu'une copie temporaire de l'objet soit disponible. Lorsqu'une copie temporaire de l'objet restauré est créée, la classe de stockage de l'objet reste la même. (Un HeadObject ou GetObjectLa demande d'opération d'API renvoie S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive comme classe de stockage.)
- Pour les objets appartenant aux niveaux d'accès Archive S3 Intelligent-Tiering et Deep Archive S3 Intelligent-Tiering, vous devez lancer la demande de restauration et attendre que l'objet soit déplacé dans le niveau d'accès Frequent.

Pour en savoir plus sur la comparaison de toutes les classes de stockage Amazon S3, consultez Bien comprendre et gérer les classes de stockage Amazon S3. Pour plus d'informations sur S3 Intelligent-Tiering, consultez the section called "Fonctionnement de S3 Intelligent-Tiering".

Le temps nécessaire à l'exécution d'une tâche de restauration dépend de la classe de stockage d'archive ou du niveau de stockage que vous utilisez et de l'option de récupération que vous spécifiez : Expédié (uniquement disponible pour S3 Glacier Flexible Retrieval et le niveau Archive Access de S3 Intelligent-Tiering), Standard ou En bloc. Pour de plus amples informations, veuillez consulter Présentation des options de récupération d'archives.

Vous pouvez être averti à l'issue de la restauration grâce aux notifications d'événements Amazon S3. Pour de plus amples informations, veuillez consulter Notifications d'événements Amazon S3.

Restauration d'objets depuis S3 Glacier

Lorsque vous utilisez S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, Amazon S3 restaure une copie temporaire de l'objet uniquement pour la durée spécifiée. Une fois ce temps écoulé, il supprime la copie de l'objet restaurée. Vous pouvez modifier la période d'expiration d'une copie restaurée en réémettant une demande de restauration. Dans ce cas, Amazon S3 met à jour la période d'expiration relative à l'heure actuelle.

> **Note**
>
> Lorsque vous restaurez un objet archivé depuis S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, vous payez à la fois pour l'objet archivé et pour la copie que vous avez restaurée temporairement. Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3.

Amazon S3 calcule le délai d'expiration de la copie d'objet restaurée en ajoutant le nombre de jours spécifié dans la demande de restauration au moment où la restauration demandée est terminée. Amazon S3 arrondit ensuite la date et l'heure obtenues au jour suivant à minuit heure UTC (Universal Coordinated Time). Par exemple, supposons qu'une copie d'objet restaurée a été créée le 15 octobre 2012 à 10h30 UTC et que la période de restauration a été spécifiée comme étant de trois jours. Dans ce cas, la copie restaurée expire le 19 octobre 2012 à minuit heure UTC, moment auquel Amazon S3 supprime la copie de l'objet.

Restauration des objets depuis S3 Intelligent-Tiering

Lorsque vous restaurez un objet à partir du niveau Archive Access de S3 Intelligent-Tiering ou du niveau Deep Archive Access de S3 Intelligent-Tiering, l'objet revient au niveau d'accès fréquent de S3 Intelligent-Tiering. Si vous n'accédez pas à l'objet dans 30 jours consécutifs, il est automatiquement déplacé vers le niveau Accès peu fréquent. Après un minimum de 90 jours consécutifs sans accès, l'objet passe au niveau Accès aux archives S3 Intelligent-Tiering. Si vous n'accédez pas à l'objet pendant un minimum de 180 jours consécutifs, il passe au niveau Accès Deep Archive.

> **Note**
>
> Contrairement aux classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive, les demandes de restauration pour les objets S3 Intelligent-Tiering n'acceptent pas la valeur `Days`.

Utilisation des opérations par lots S3 avec les demandes de restauration

Pour restaurer plusieurs objets Amazon S3 avec une seule demande, vous pouvez utiliser la fonctionnalité d'opérations par lots S3. Vous fournissez à la fonctionnalité d'opérations par lots S3 une liste d'objets sur lesquels effectuer des opérations. La fonctionnalité des opérations par lot S3 appelle l'opération d'API respective pour effectuer l'opération spécifiée. Une tâche d'opérations par lot peut effectuer l'opération spécifiée sur des milliards d'objets contenant des exaoctets de données.

Rubriques

- Présentation des options de récupération d'archives
- Restauration d'un objet archivé

Présentation des options de récupération d'archives

Voici les opérations relatives aux options de récupération lors de la restauration d'un objet archivé dans Amazon S3 :

- Expédié : accédez rapidement à vos données stockées dans la classe de stockage S3 Glacier Flexible Retrieval ou au niveau Archive Access de S3 Intelligent-Tiering. Vous pouvez utiliser cette option lorsque des demandes urgentes occasionnelles concernant un sous-ensemble d'archives sont nécessaires. Pour tous les objets archivés, à l'exception des plus volumineux (plus de 250 Mo), les données auxquelles vous accédez à l'aide des récupérations rapides sont généralement disponibles en 1 à 5 minutes.

  > **Note**
  >
  > Les récupérations accélérées sont une fonctionnalité premium et sont facturées au tarif des demandes et des récupérations accélérées.
  > Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

  La capacité provisionnée aide à garantir que la capacité de récupération pour les récupérations rapides de S3 Glacier Flexible Retrieval est disponible lorsque vous en avez besoin. Pour de plus amples informations, veuillez consulter Capacité provisionnée.
- Standard : accédez à tous vos objets archivés en quelques heures. Standard constitue l'option par défaut pour les demandes de récupération qui ne spécifient pas l'option de récupération. Les récupérations standard prennent généralement 3 à 5 heures pour les objets stockés dans la classe de stockage S3 Glacier Flexible Retrieval ou dans le niveau d'accès Archive de S3 Intelligent-Tiering. Ces récupérations se terminent généralement en 12 heures pour les objets stockés dans la classe de stockage S3 Glacier Deep Archive ou au niveau d'accès Deep Archive de S3 Intelligent-Tiering. Les récupérations standard sont gratuites pour les objets stockés dans S3 Intelligent-Tiering.

  > **Note**
  >
  > - Pour les objets stockés dans la classe de stockage S3 Glacier Flexible Retrieval ou au niveau Archive Access de S3 Intelligent-Tiering, les récupérations standard lancées via l'opération de restauration des opérations par lot S3 commencent généralement au bout de quelques minutes et prennent entre 3 et 5 heures.

- Pour les objets figurant dans la classe de stockage S3 Glacier Deep Archive ou au niveau Deep Archive Access de S3 Intelligent-Tiering, les récupérations standard lancées via l'opération de restauration Opérations par lot commencent généralement dans les 9 heures et se terminent dans les 12 heures.

- En bloc : accédez à vos données avec l'option de récupération la moins coûteuse dans Amazon S3 Glacier. Avec les récupérations en bloc, vous pouvez récupérer de grandes quantités de données, même des pétaoctets, à moindre coût.

  Pour les objets stockés dans la classe de stockage S3 Glacier Flexible Retrieval ou au niveau Archive Access de S3 Intelligent-Tiering, les récupérations en bloc se terminent généralement dans les 5 à 12 heures. Pour les objets stockés dans la classe de stockage S3 Glacier Deep Archive ou au niveau Deep Archive Access de S3 Intelligent-Tiering, les récupérations se terminent généralement dans les 48 heures.

  Les récupérations en bloc sont gratuites pour les objets stockés dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Intelligent-Tiering.

Le tableau suivant récapitule les options de récupération d'archive. Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3.

Pour effectuer une ou une `Bulk` extraction `ExpeditedStandard`, définissez l'élément de `Tier` demande dans le RestoreObjectDemande d'opération de l'API REST à l'option que vous souhaitez, ou à l'option équivalente dans le AWS Command Line Interface (AWS CLI) ou AWS SDKs. Si vous avez acheté une capacité provisionnée, toutes les récupérations rapides de type Expedited sont automatiquement transmises par le biais de votre capacité provisionnée.

Capacité provisionnée

La capacité provisionnée aide à garantir que votre capacité de récupération pour les récupérations accélérées depuis S3 Glacier Flexible Retrieval est disponible lorsque vous en avez besoin. Chaque unité de capacité permet d'effectuer au moins trois extractions accélérées toutes les 5 minutes, et fournit un débit de récupération allant jusqu'à 150 mégaoctets par seconde (). MBps

Si votre charge de travail nécessite un accès extrêmement fiable et prévisible à un sous-ensemble de vos données en quelques minutes, envisagez d'acheter une capacité de récupération provisionnée. Sans capacité provisionnée, les récupérations accélérées peuvent ne pas être acceptées lors de périodes de demandes élevées. Si vous avez besoin d'un accès aux récupérations accélérées

en toutes circonstances, nous vous recommandons d'acheter de la capacité de récupération provisionnée.

Les unités de capacité allouées sont allouées à un Compte AWS. Ainsi, le demandeur de la récupération accélérée des données doit acheter l'unité de capacité provisionnée, et non pas le propriétaire du compartiment.

Vous pouvez acheter de la capacité provisionnée à l'aide de la console Amazon S3, de la console Amazon S3 Glacier, de l'opération d'API REST Purchase Provisioned Capacity AWS SDKs, du ou du. AWS CLI Pour de plus amples informations sur la tarification de la capacité provisionnée, consultez Tarification Amazon S3.

Taux de demandes d'initiation de restauration S3 Glacier

Lorsque vous lancez des demandes de restauration pour des objets stockés dans la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, un quota de demandes de récupération est appliqué pour votre Compte AWS. S3 Glacier prend en charge les demandes de restauration à un débit allant jusqu'à 1 000 transactions par seconde. Si ce taux est dépassé, des demandes valides sont limitées ou rejetées et Amazon S3 renvoie une erreur `ThrottlingException`.

En option, vous pouvez également utiliser les opérations par lots S3 pour récupérer un grand nombre d'objets stockés dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive avec une demande simple. Pour de plus amples informations, veuillez consulter Exécution d'opérations groupées sur des objets avec les opérations par lot.

Restauration d'un objet archivé

Les objets Amazon S3 figurant dans les classes ou niveaux de stockage suivants sont archivés et ne sont pas accessibles en temps réel :

- Classe de stockage S3 Glacier Flexible Retrieval
- Classe de stockage S3 Glacier Deep Archive
- Niveau Accès aux archives S3 Intelligent-Tiering.
- Niveau d'accès Deep Archive de S3 Intelligent-Tiering

Les objets Amazon S3 stockés dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive ne sont pas immédiatement accessibles. Pour accéder à un objet dans ces classes de stockage, vous devez en restaurer une copie temporaire de l'objet dans

son compartiment S3 pendant une durée spécifiée (nombre de jours). Si vous souhaitez une copie permanente de l'objet, restaurez l'objet, puis créez-en une copie dans votre compartiment Amazon S3. La copie des objets restaurés n'est pas prise en charge dans la console Amazon S3. Pour ce type d'opération de copie, utilisez l'API AWS Command Line Interface (AWS CLI) AWS SDKs, l'API ou l'API REST. Excepté dans le cas où vous effectuez une copie et modifiez sa classe de stockage, l'objet sera toujours stocké dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour obtenir des informations sur l'utilisation de ces classes de stockage, consultez Classes de stockage pour les objets rarement consultés.

Pour accéder aux objets dans les niveaux Archive Access et Deep Archive Access de S3 Intelligent-Tiering, vous devez lancer une demande de restauration, puis attendre que l'objet soit placé au niveau d'accès fréquent. Lorsque vous restaurez un objet depuis les niveaux d'accès Archive et Deep Archive, l'objet retourne au niveau d'accès Fréquent. Pour obtenir des informations sur l'utilisation de ces classes de stockage, consultez Classe de stockage pour l'optimisation automatique des données avec des modèles d'accès inconnus ou irréguliers.

Pour obtenir des informations générales sur les objets archivés, consultez Utilisation des objets archivés.

> **Note**
>
> - Lorsque vous restaurez un objet archivé à partir des classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, vous payez à la fois pour l'objet archivé et pour la copie que vous restaurez temporairement.
> - Lorsque vous restaurez un objet à partir de S3 Intelligent-Tiering, aucun frais de récupération n'est facturé pour les récupérations standard ou en bloc.
> - Les demandes de restauration ultérieures appelées sur des objets archivés qui ont déjà été restaurés sont facturées en tant que demandes `GET`. Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3.

Restauration d'un objet archivé

Vous pouvez restaurer un objet archivé à l'aide de la console Amazon S3, de l'API REST Amazon S3 AWS SDKs, des opérations par lots, the AWS Command Line Interface (AWS CLI) ou S3 Batch.

Utilisation de la console S3

Restauration d'objets à l'aide de la console Amazon S3

Utilisez la procédure suivante pour restaurer un objet qui a été archivé dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, ou aux niveaux de stockage Archive Access ou Deep Archive Access de S3 Intelligent-Tiering.

Pour restaurer un objet archivé

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des buckets, choisissez le nom du bucket qui contient les objets que vous souhaitez restaurer.
4. Dans la liste Objets, sélectionnez le ou les objets à restaurer, choisissez Actions, puis Lancer la restauration.
5. Si vous effectuez une restauration depuis S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, saisissez le nombre de jours pendant lesquels vous souhaitez que vos données archivées soient accessibles dans la zone Nombre de jours pendant lesquels la copie restaurée est disponible.
6. Dans Niveau d'extraction, effectuez l'une des opérations suivantes :

   - Choisissez Récupération en bloc ou Récupération standard, puis Commencer la restauration.
   - Choisissez Récupération accélérée (disponible uniquement pour S3 Glacier Flexible Retrieval ou l'accès Archive de S3 Intelligent-Tiering). Si vous restaurez un objet dans S3 Glacier Flexible Retrieval, vous pouvez choisir d'acheter une capacité provisionnée pour votre récupération accélérée. Si vous souhaitez acheter une capacité provisionnée, passez à l'étape suivante. Si ce n'est pas le cas, choisissez Commencer la restauration.

   > **Note**
   >
   > Les objets des niveaux Archive Access et Deep Archive Access de S3 Intelligent-Tiering sont restaurés automatiquement au niveau d'accès fréquent.

7. (Facultatif) Si vous restaurez un objet dans S3 Glacier Flexible Retrieval et que vous avez choisi Récupération accélérée, vous pouvez choisir d'acheter une capacité provisionnée. La capacité provisionnée n'est disponible que pour les objets se trouvant dans S3 Glacier Flexible Retrieval. Si vous disposez d'une capacité provisionnée, choisissez Commencer la restauration pour démarrer une récupération provisionnée.

Si vous disposez d'une capacité provisionnée, toutes vos récupérations accélérées sont effectuées avec votre capacité provisionnée. Pour de plus amples informations, veuillez consulter Capacité provisionnée.

- Si vous ne disposez pas d'une capacité provisionnée et que vous ne voulez pas en acheter, choisissez Commencer la restauration.
- Si vous ne disposez pas de capacité provisionnée, mais que vous souhaitez acheter des unités de capacité provisionnées (PCUs), choisissez Acheter. PCUs Dans la boîte PCUs de dialogue d'achat, choisissez le nombre que PCUs vous souhaitez acheter, confirmez votre achat, puis choisissez Acheter PCUs. Lorsque le message Réussite de l'achat s'affiche, choisissez Commencer la restauration pour démarrer la récupération provisionnée.

À l'aide du AWS CLI

Restauration d'objets depuis S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive

L'exemple suivant utilise la commande `restore-object` pour restaurer l'objet *dir1/example.obj* dans le compartiment *amzn-s3-demo-bucket*pendant 25 jours.

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{"Days":25,"GlacierJobParameters":{"Tier":"Standard"}}'
```

Si la syntaxe JSON utilisée dans cet exemple génère une erreur sur un client Windows, remplacez la demande de restauration par la syntaxe suivante :

```
--restore-request Days=25,GlacierJobParameters={"Tier"="Standard"}
```

Restauration d'objets depuis le niveau Archive Access ou Deep Archive Access de S3 Intelligent-Tiering

L'exemple suivant utilise la commande `restore-object` pour restaurer l'objet *dir1/example.obj* dans le compartiment *amzn-s3-demo-bucket* au niveau d'accès fréquent.

```
aws s3api restore-object --bucket amzn-s3-demo-bucket --key dir1/example.obj --restore-request '{}'
```

> **Note**
>
> Contrairement aux classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive, les demandes de restauration pour les objets S3 Intelligent-Tiering n'acceptent pas la valeur `Days`.

Surveillance du statut de la restauration

Pour surveiller le statut de votre demande `restore-object`, utilisez la commande suivante `head-object` :

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

Pour plus d'informations, consultez .restore-objectdans la référence de AWS CLI commande.

Utilisation de l'API REST

Amazon S3 fournit une opération d'API pour vous permettre de lancer la restauration d'un objet archivé. Pour plus d'informations, consultez .RestoreObjectdans le manuel Amazon Simple Storage Service API Reference.

À l'aide du AWS SDKs

Pour des exemples de restauration d'objets archivés dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive avec le AWS SDKs, consultez les exemples de code dans le manuel Amazon S3 API Reference.

Utilisation des opérations par lot S3

Pour restaurer plusieurs objets archivés avec une seule demande, vous pouvez utiliser les opérations par lot S3. Vous fournissez à la fonctionnalité d'opérations par lots S3 une liste d'objets sur lesquels effectuer des opérations. La fonctionnalité des opérations par lot S3 appelle l'opération d'API respective pour effectuer l'opération spécifiée. Une tâche d'opérations par lot peut effectuer l'opération spécifiée sur des milliards d'objets contenant des exaoctets de données.

Pour créer une tâche d'opérations par lot, vous devez disposer d'un manifeste contenant uniquement les objets que vous souhaitez restaurer. Vous pouvez créer un manifeste à l'aide de S3 Inventory ou vous pouvez fournir un fichier CSV contenant les informations nécessaires. Pour de plus amples informations, veuillez consulter the section called "Spécification d'un manifeste".

Avant de créer et d'exécuter des tâches d'opérations par lot S3, vous devez accorder des autorisations à Amazon S3 pour effectuer des opérations par lot S3 en votre nom. Pour les autorisations requises, consultez the section called "Octroi d'autorisations".

> **Note**
>
> Les tâches d'opérations par lot peuvent fonctionner sur les objets de classe de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive, ou sur les objets des niveaux de stockage Archive Access et Deep Archive Access de S3 Intelligent-Tiering. Les opérations par lot ne peuvent pas fonctionner sur les deux types d'objets archivés dans la même tâche. Pour restaurer des objets des deux types, vous devez créer des tâches Batch Operations. Pour plus d'informations sur l'utilisation des opérations par lot pour restaurer des objets archivés, consultez the section called "Restaurer des objets".

Pour créer une tâche d'opérations par lot Lancer une restauration d'objet S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Opérations par lot.
3. Choisissez Créer une tâche.
4. Pour Région AWS, choisissez la Région dans laquelle vous souhaitez créer votre tâche.
5. Sous Format du manifeste, choisissez le type de manifeste à utiliser.
   - Si vous choisissez Rapport d'inventaire S3, entrez le chemin d'accès de l'objet `manifest.json` généré par Amazon S3 dans le cadre du rapport d'inventaire au format CSV. Si vous souhaitez utiliser une version de manifeste autre que la plus récente, saisissez l'ID de version de l'objet `manifest.json`.
   - Si vous choisissez CSV, entrez le chemin vers un objet manifeste au format CSV. L'objet manifeste doit respecter le format décrit dans la console. Si vous souhaitez utiliser une version autre que la plus récente, vous pouvez éventuellement inclure l'ID de version de l'objet manifeste.
6. Choisissez Suivant.
7. Dans la section Opération, choisissez Restaurer.
8. Dans la section Restaurer, pour Restaurer la source, choisissez Glacier Flexible Retrieval ou Glacier Deep Archive ou Niveau Archive Access ou Deep Archive Access d'Intelligent-Tiering.

Si vous avez choisi Glacier Flexible Retrieval ou Glacier Deep Archive, entrez un nombre pour Nombre de jours pendant lesquels la copie restaurée est disponible.

Pour Niveau d'extraction, choisissez le niveau que vous souhaitez utiliser.

9. Choisissez Suivant.

10. Sur la page Configurer des options supplémentaires, remplissez les sections suivantes :

    - Dans la section Options supplémentaires, fournissez une description de la tâche et spécifiez un numéro de priorité pour la tâche. Un nombre plus élevé indique une priorité plus élevée. Pour de plus amples informations, veuillez consulter the section called "Affectation d'une priorité de tâche".
    - Dans la section Rapport d'achèvement, sélectionnez si les opérations par lot doivent créer un rapport d'achèvement. Pour plus d'informations sur les rapports d'achèvement, consultez the section called "Rapports de fin de tâche".
    - Dans la section Autorisations, vous devez accorder des autorisations à Amazon S3 pour effectuer des opérations par lot en votre nom. Pour les autorisations requises, consultez the section called "Octroi d'autorisations".
    - (Facultatif) Dans la section Balises de tâche, ajoutez des balises dans les paires clé-valeur. Pour de plus amples informations, veuillez consulter the section called "Utilisation d'étiquettes".

    Lorsque vous avez terminé, choisissez Suivant.

11. Sur la page Vérification, vérifiez les paramètres. Si vous devez apporter des modifications, choisissez Précédent. Sinon, choisissez Créer une tâche.

Pour plus d'informations sur les opérations par lot, consultez Restauration d'objets à l'aide d'opérations par lot et Création d'une tâche d'opérations par lot S3.

Vérification du statut et de la date d'expiration de la restauration

Vous pouvez vérifier l'état d'une demande de restauration ou sa date d'expiration à l'aide de la console Amazon S3, des notifications d'événements Amazon S3, de l' AWS CLI API REST Amazon S3 ou de l'API REST Amazon S3.

> **Note**
>
> Les objets restaurés à partir des classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive sont stockés uniquement pendant le nombre de jours que vous spécifiez. Les procédures suivantes renvoient la date d'expiration de ces copies.
> Les objets restaurés à partir des niveaux de stockage Archive Access ou Deep Archive Access de S3 Intelligent-Tiering n'ont pas de date d'expiration et sont renvoyés au niveau d'accès fréquent.

Utilisation de la console S3

Pour vérifier le statut de la restauration et la date d'expiration d'un objet dans la console Amazon S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des buckets, choisissez le nom du bucket qui contient l'objet que vous restaurez.
4. Dans la liste Objets, sélectionnez l'objet que vous êtes en train de restaurer. La page de détails de l'objet s'affiche.

    - Si la restauration n'est pas terminée, en haut de la page, vous voyez une section qui stipule Restauration en cours.
    - Si la restauration est terminée, en haut de la page, vous voyez une section qui stipule Restauration terminée. Si vous effectuez une restauration depuis S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, cette section affiche également la Date d'expiration de la restauration. Amazon S3 supprimera à cette date la copie restaurée de votre objet archivé.

Utilisation des notifications d'événements Amazon S3

Vous pouvez être averti par notification de la fin de la restauration d'un objet en utilisant l'action `s3:ObjectRestore:Completed` avec la fonctionnalité Notifications d'événements Amazon S3. Pour plus d'informations sur l'activation des notifications d'événements, consultez Activation des notifications à l'aide d'Amazon SQS, Amazon SNS et. AWS Lambda Pour plus d'informations sur les divers types d'événements `ObjectRestore`, consultez the section called "Types d'événements pris en charge pour SQS, SNS et Lambda".

À l'aide du AWS CLI

Vérifiez l'état de restauration et la date d'expiration d'un objet à l'aide du AWS CLI

L'exemple suivant utilise la commande `head-object` pour afficher les métadonnées de l'objet *`dir1/example.obj`* dans le compartiment *`amzn-s3-demo-bucket`*. Lorsque vous exécutez cette commande sur un objet en cours de restauration, Amazon S3 indique si la restauration est en cours et (le cas échéant) la date d'expiration.

```
aws s3api head-object --bucket amzn-s3-demo-bucket --key dir1/example.obj
```

Résultat attendu (restauration en cours) :

```
{
    "Restore": "ongoing-request=\"true\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

Résultat attendu (restauration terminée) :

```
{
    "Restore": "ongoing-request=\"false\", expiry-date=\"Wed, 12 Aug 2020 00:00:00 GMT
\"",
    "LastModified": "2020-06-16T21:55:22+00:00",
    "ContentLength": 405,
    "ETag": "\"b662d79adeb7c8d787ea7eafb9ef6207\"",
    "VersionId": "wbYaE2vtOV0iIBXrOqGAJt3fP1cHB8Wi",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "AES256",
    "Metadata": {},
    "StorageClass": "GLACIER"
}
```

Pour plus d'informations sur `head-object`, consultez .head-objectdans la référence de AWS CLI commande.

Utilisation de l'API REST

Amazon S3 fournit une opération d'API qui vous permet de récupérer les métadonnées des objets. Pour vérifier l'état de restauration et la date d'expiration d'un objet archivé à l'aide de l'API REST, voir HeadObjectdans le manuel Amazon Simple Storage Service API Reference.

Mise à niveau de la vitesse d'une restauration en cours

Vous pouvez mettre à niveau la vitesse de la restauration pendant que cette dernière est en cours.

Pour mettre à niveau une restauration en cours vers un niveau plus rapide

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le nom du compartiment qui contient les objets que vous souhaitez restaurer.
4. Dans la liste Objets, sélectionnez l'objet que vous êtes en train de restaurer. La page de détails de l'objet s'affiche. Sur la page de détails de l'objet, choisissez Mettre à niveau le niveau d'extraction. Pour de plus amples informations sur la vérification du statut de restauration d'un objet, consultez Vérification du statut et de la date d'expiration de la restauration.
5. Choisissez le niveau auquel vous souhaitez passer, puis choisissez Commencer la restauration.

Gestion du cycle de vie des objets

Le cycle de vie S3 vous aide à stocker les objets de manière économique tout au long de leur cycle de vie en les transférant vers des classes de stockage moins coûteuses ou en supprimant les objets expirés en votre nom. Pour gérer le cycle de vie de vos objets, créez une configuration du cycle de vie S3 pour votre compartiment. Une configuration de cycle de vie S3 est un ensemble de règles qui définit des actions qu'Amazon S3 applique à un groupe d'objets. Il existe deux types d'actions :

- Actions de transition : ces actions définissent à quel moment les objets effectuent la transition vers une autre classe de stockage. Par exemple, vous pouvez choisir d'effectuer la transition des objets vers la classe de stockage S3 standard – Accès peu fréquent 30 jours après leur création ou de les archiver dans la classe de stockage S3 Glacier Flexible Retrieval un an après leur création. Pour plus d'informations, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

  Des coûts sont associés aux demandes de transition de cycle de vie. Pour en savoir plus sur la tarification, consultez Tarification Amazon S3.

- Actions d'expiration : ces actions définissent la date d'expiration des objets. Amazon S3 supprime les objets expirés à votre place. Par exemple, vous pouvez choisir de faire expirer les objets après leur stockage pendant une période de conformité réglementaire. Pour de plus amples informations, veuillez consulter Objets en cours d'expiration.

  Des coûts potentiels sont associés à l'expiration du cycle de vie uniquement lorsque vous faites expirer des objets figurant dans une classe de stockage avec une durée de stockage minimale. Pour de plus amples informations, veuillez consulter Frais de durée minimale de stockage.

> **Important**
>
> Compartiments à usage général : vous ne pouvez pas utiliser une politique de compartiment pour empêcher les suppressions ou les transitions selon une règle du cycle de vie S3. Par exemple, même si votre politique de compartiment refuse toutes les actions pour tous les principaux, votre configuration du cycle de vie S3 continue de fonctionner normalement.

Objets existants et nouveaux

Quand vous ajoutez une configuration de cycle de vie dans un compartiment, les règles de configuration s'appliquent à la fois aux objets existants et à ceux que vous ajouterez ultérieurement. À titre d'exemple, si vous ajoutez aujourd'hui une règle de configuration du cycle de vie avec une action d'expiration qui fait expirer les objets 30 jours après leur création, Amazon S3 met en file d'attente de suppression tous les objets existants qui datent de plus de 30 jours.

Changements au niveau de la facturation

En cas de retard entre le moment où un objet devient éligible à une action de cycle de vie et le moment où Amazon S3 transfère ou fait expirer votre objet, les modifications de facturation sont appliquées dès que l'objet devient éligible à l'action de cycle de vie. Par exemple, si l'expiration d'un objet est planifiée et qu'Amazon S3 ne le fait pas expirer immédiatement, le stockage ne vous sera pas facturé après la date d'expiration.

Il existe toutefois une exception à ce comportement si vous disposez d'une règle de cycle de vie configurée pour transférer l'objet à la classe de stockage S3 Intelligent-Tiering. Dans ce cas, les changements de facturation ne se produisent pas tant que l'objet n'est pas passé à la classe de stockage S3 Intelligent-Tiering. Pour plus d'informations sur les règles de cycle de vie S3, consultez Éléments de la configuration du cycle de vie.

> **Note**
>
> Aucuns frais de récupération de données ne s'appliquent pour les transitions de cycle de vie. Toutefois, des frais d'ingestion par demande s'appliquent lors de l'utilisation de PUT, de COPY ou de règles de cycle de vie pour placer des données dans une classe de stockage S3 quelconque. Tenez compte du coût d'ingestion ou de transition avant de placer des objets dans une classe de stockage quelconque. Pour plus d'informations sur les coûts, consultez Tarification Amazon S3.

Surveillance de l'effet des règles de cycle de vie

Pour surveiller l'effet des mises à jour effectuées par les règles de cycle de vie actives, consultez the section called "Comment puis-je surveiller les actions prises conformément à mes règles de cycle de vie ?".

Gestion du cycle de vie complet des objets

Les règles de configuration du cycle de vie S3 vous permettent d'indiquer à Amazon S3 d'effectuer la transition des objets vers des classes de stockage moins coûteuses, de les archiver ou de les supprimer. Par exemple :

- Si vous chargez régulièrement des journaux dans votre compartiment, il se peut que l'application ait besoin de ces journaux pendant une semaine ou un mois. À l'issue de cette période, vous pouvez souhaiter les supprimer.
- Certains documents sont consultés fréquemment pendant une période limitée. À l'issue de cette période, ils sont moins souvent consultés. À un moment donné, il est possible que vous n'ayez pas besoin d'y accéder en temps réel, mais votre entreprise ou la législation peut vous imposer de les archiver pour une durée spécifique. À l'issue de cette période, vous pouvez les supprimer.
- Vous pouvez télécharger certains types de données sur Amazon S3, essentiellement à des fins d'archivage. Par exemple, vous pouvez archiver des médias numériques, des dossiers financiers et médicaux, des données brutes de séquences génomiques, des sauvegardes de bases de données à long terme et des données à conserver pour des raisons de conformité réglementaire.

En combinant les actions de cycle de vie S3 pour gérer le cycle de vie complet d'un objet. Par exemple, admettons que les objets que vous créez ont un cycle de vie bien défini. À la base, les objets sont utilisés fréquemment pendant une période de 30 jours. Ensuite, les objets font

l'objet d'accès peu fréquents pendant une période de 90 jours. Par la suite, les objets ne sont plus nécessaires, vous pouvez donc décider de les archiver ou de les supprimer.

Dans ce scénario, vous pouvez créer une règle de cycle de vie S3 vous permettant de spécifier l'action de transition initiale vers la classe de stockage S3 Intelligent-Tiering, S3 Standard-IA ou S3 One Zone-IA, une autre action de transition vers la classe de stockage S3 Glacier Flexible Retrieval à des fins d'archivage et une action d'expiration. Lorsque vous déplacez les objets d'une classe de stockage à une autre, vous économisez sur les coûts de stockage. Pour plus d'informations sur les coûts, consultez Tarification Amazon S3.

Rubriques

- Transition des objets à l'aide du cycle de vie Amazon S3
- Objets en cours d'expiration
- Définition d'une configuration du cycle de vie S3 sur un compartiment
- Comment le cycle de vie S3 interagit avec d'autres configurations de compartiments
- Configuration des notifications d'événements du cycle de vie S3
- Éléments de la configuration du cycle de vie
- Comment Amazon S3 gère les conflits dans les configurations du cycle de vie
- Exemples de configurations du cycle de vie S3
- Résolution des problèmes du cycle de vie Amazon S3

Transition des objets à l'aide du cycle de vie Amazon S3

Vous pouvez ajouter des actions de transition à une configuration du cycle de vie S3 afin d'indiquer à Amazon S3 de déplacer des objets vers une autre classe de stockage Amazon S3. Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3. Voici quelques exemples de situations où vous pouvez utiliser les configurations du cycle de vie S3 de cette manière :

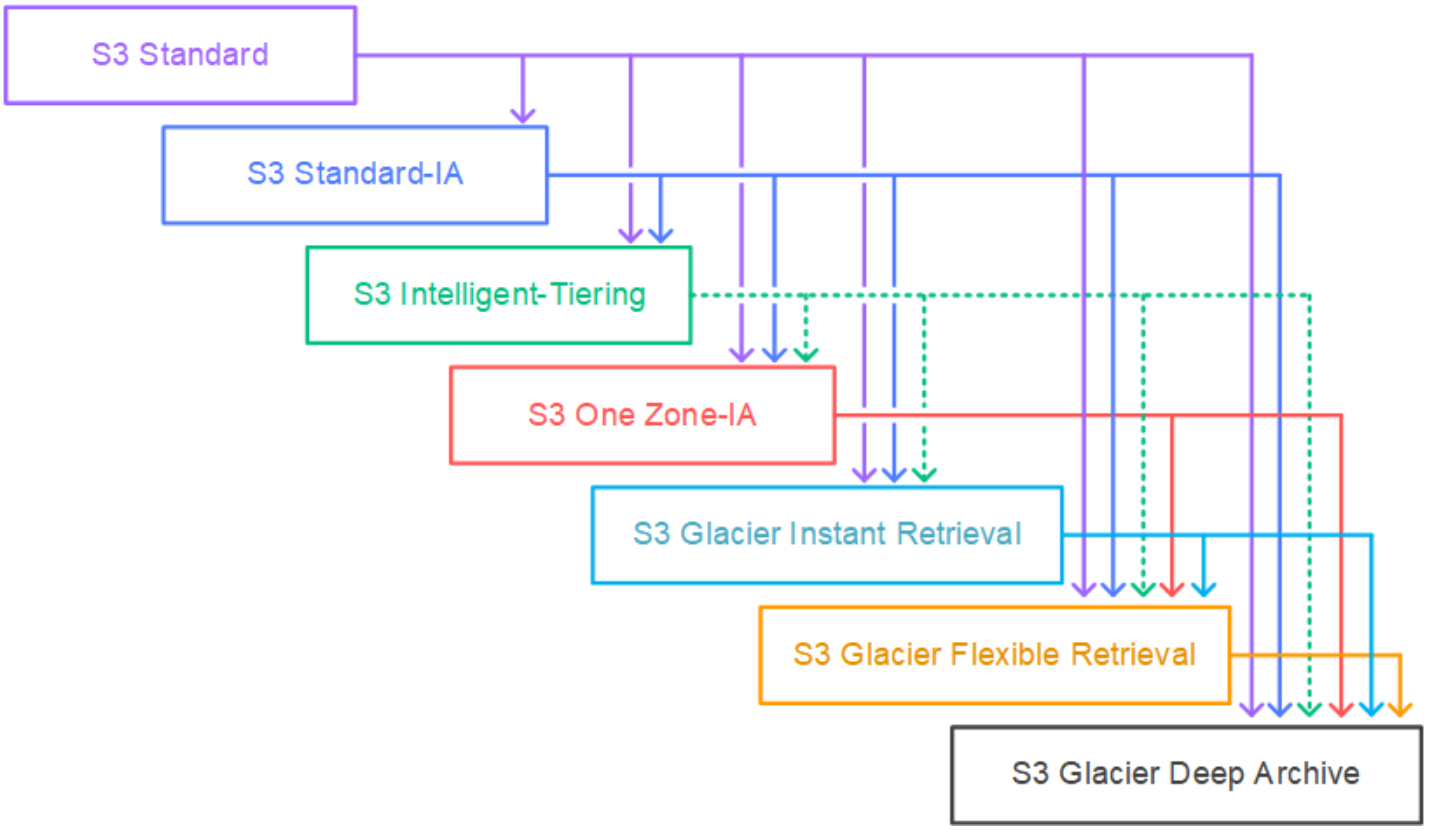
- Lorsque vous savez qu'il s'agit d'objets à accès peu fréquent, vous pouvez effectuer leur transition vers la classe de stockage S3 standard – Accès peu fréquent.
- Vous pouvez choisir d'archiver les objets auxquels vous n'avez pas besoin d'accéder en temps réel dans la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.

> **Note**
>
> Les objets chiffrés restent chiffrés tout au long du processus de transition de la classe de stockage.

Transitions prises en charge

Dans une configuration de cycle de vie S3, vous pouvez définir des règles afin d'effectuer la transition d'objets d'une classe de stockage vers une autre et économiser les coûts de stockage. Si vous ne connaissez pas les modèles d'accès de vos objets ou que vos modèles d'accès évoluent au fil du temps, vous pouvez effectuer la transition des objets vers la classe de stockage S3 Intelligent-Tiering pour réduire automatiquement les coûts. Pour obtenir des informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3.

Amazon S3 prend en charge un modèle en cascade pour la transition entre classes de stockage, comme illustré dans le schéma suivant.



Transitions de cycle de vie prises en charge

Amazon S3 prend en charge les transitions de cycle de vie suivantes entre les classes de stockage à l'aide d'une configuration de cycle de vie S3.

- La classe de stockage S3 Standard correspond aux classes de stockage S3 Standard-IA, S3 Intelligent-Tiering, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- La classe de stockage S3 Standard-IA vers les classes de stockage S3 Intelligent-Tiering, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- La classe de stockage S3 Intelligent-Tiering peut passer à différentes classes de stockage en fonction du niveau d'accès S3 Intelligent-Tiering. Les transitions suivantes sont possibles pour chaque niveau d'accès.
  - Niveau d'accès fréquent ou niveau d'accès peu fréquent aux classes de stockage S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
  - Niveau Archive Instant Access pour les classes de stockage S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
  - Niveau d'accès aux archives pour les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
  - Niveau Deep Archive Access pour les classes de stockage S3 Glacier Deep Archive.
- La classe de stockage S3 One Zone-IA vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- La classe de stockage S3 Glacier Instant Retrieval vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive.
- La classe de stockage S3 Glacier Flexible Retrieval vers la classe de stockage S3 Glacier Deep Archive.

> **Note**
>
> Pour le versionnement activé ou le versionnement des buckets suspendus, vous ne pouvez pas transférer des objets dotés d'un `Pending` statut de réplication.

Contraintes et considérations pour les transitions

Les transitions des classes de stockage de cycle de vie obéissent aux contraintes suivantes :

Les objets de moins de 128 Ko ne sont pas transférés par défaut vers une classe de stockage

Amazon S3 applique un comportement par défaut à vos configurations du cycle de vie S3 qui empêche la transition des objets de moins de 128 Ko vers toute classe de stockage. Nous ne recommandons pas de transférer des objets de moins de 128 Ko, car une demande de transition vous est facturée pour chaque objet. Cela signifie que pour les objets plus petits, les coûts de transition peuvent l'emporter sur les économies de stockage. Pour plus d'informations sur les coûts des demandes de transition, consultez Demandes et extractions de données dans l'onglet Stockage et demandes de la page Tarification Amazon S3.

Pour permettre la transition entre des objets plus petits, vous pouvez ajouter un filtre de taille d'objet à vos règles de transition du cycle de vie, qui spécifie une taille minimale (`ObjectSizeGreaterThan`) ou maximale (`ObjectSizeLessThan`) personnalisée. Pour de plus amples informations, veuillez consulter Exemple : permettre la transition d'objets de moins de 128 Ko.

> **Note**
>
> En septembre 2024, Amazon S3 a mis à jour le comportement de transition par défaut pour les petits objets, comme suit :
>
> - Comportement de transition par défaut mis à jour : à compter du mois de septembre 2024, le comportement par défaut empêche les objets de moins de 128 Ko d'être transférés vers toute classe de stockage.
> - Comportement de transition par défaut précédent : avant le mois de septembre 2024, le comportement par défaut autorisait les objets de moins de 128 Ko à être transférés uniquement vers les classes de stockage S3 Glacier et S3 Glacier Deep Archive.
>
> Les configurations créées avant le mois de septembre 2024 conservent le comportement de transition précédent, sauf si vous les modifiez. En d'autres termes, si vous créez, modifiez ou supprimez des règles, le comportement de transition par défaut de votre configuration est remplacé par le comportement mis à jour. Si votre cas d'utilisation l'exige, vous pouvez modifier le comportement de transition par défaut afin que les objets de moins de 128 Ko soient transférés vers S3 Glacier et S3 Glacier Deep Archive. Pour ce faire, utilisez l'`x-amz-transition-default-minimum-object-size`en-tête facultatif dans une PutBucketLifecycleConfigurationdemande.

Les objets doivent être stockés au moins 30 jours avant d'être transférés vers S3 Standard-IA ou S3 One Zone-IA

Avant d'effectuer la transition d'objets vers les classes de stockage S3 Standard-IA ou S3 One Zone-IA, vous devez les stocker au moins 30 jours dans Amazon S3. Par exemple, vous ne pouvez pas créer une règle de cycle de vie pour effectuer la transition d'objets vers la classe de stockage S3 standard – Accès peu fréquent un jour après leur création. Amazon S3 ne prend pas en charge cette transition dans les 30 premiers jours, car les objets les plus récents font souvent l'objet d'un accès plus fréquent ou sont supprimés plus rapidement comparés aux classes de stockage S3 Standard-IA ou S3 One Zone-IA.

De même, si vous effectuez la transition d'objets anciens (dans des compartiments prenant en charge la gestion des versions), vous ne pouvez effectuer la transition que d'objets anciens d'au moins 30 jours vers une classe de stockage S3 Standard-IA ou S3 One Zone-IA. Pour obtenir la liste des durées de stockage minimales pour toutes les classes de stockage, consultez Comparaison des classes de stockage Amazon S3.

La transition des objets avant leur durée de stockage minimale vous est facturée

Certaines classes de stockage ont une durée de stockage minimale des objets. Si vous retirez des objets de ces classes de stockage avant la durée minimale, le reste de cette durée vous est facturé. Pour plus d'informations sur les classes de stockage dont la durée de stockage est minimale, consultez Comparaison des classes de stockage Amazon S3.

Vous ne pouvez pas créer une règle de cycle de vie unique qui fasse passer les objets d'une classe de stockage à une autre avant que la durée de stockage minimale ne soit écoulée.

Par exemple, S3 Glacier Instant Retrieval a une durée de stockage minimale de 90 jours. Vous ne pouvez pas spécifier une règle de cycle de vie qui transfère les objets vers S3 Glacier Instant Retrieval au bout de 4 jours, puis vers S3 Glacier Deep Archive après 20 jours. Dans ce cas, la transition vers S3 Glacier Deep Archive doit avoir lieu au bout d'au moins 94 jours.

Vous pouvez spécifier deux règles pour y parvenir, mais vous payez les frais de stockage pour la durée minimale. Pour plus d'informations sur les coûts, consultez Tarification Amazon S3.

Pour plus d'informations sur la création d'un cycle de vie S3, consultez Définition d'une configuration du cycle de vie S3 sur un compartiment.

Transition vers les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive (archivage d'objets)

À l'aide de la configuration du cycle de vie S3, vous pouvez transférer les objets vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive pour les archiver.

Avant d'archiver des objets, passez en revue les sections suivantes contenant des considérations pertinentes.

Considérations d'ordre général

Les considérations générales suivantes sont à prendre en compte avant d'archiver des objets :

- Les objets chiffrés restent chiffrés tout au long du processus de transition de la classe de stockage.
- Les objets stockés dans les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive ne sont pas disponibles en temps réel.

  Les objets archivés sont des objets Amazon S3, mais avant de pouvoir accéder à un objet archivé, vous devez d'abord en restaurer une copie temporaire. La copie restaurée de l'objet est disponible uniquement pendant la durée que vous spécifiez dans la demande de restauration. Après quoi, Amazon S3 supprime la copie temporaire et l'objet reste archivé dans Amazon S3 Glacier Flexible Retrieval.

  Vous pouvez restaurer un objet à l'aide de la console Amazon S3 ou par programmation en utilisant les bibliothèques d'encapsulation du AWS SDK ou l'API REST Amazon S3 dans votre code. Pour de plus amples informations, veuillez consulter Restauration d'un objet archivé.
- Les objets stockés dans la classe de stockage S3 Glacier Flexible Retrieval peuvent uniquement faire l'objet d'une transition vers la classe de stockage S3 Glacier Deep Archive.

  Vous pouvez utiliser une règle de configuration de cycle de vie S3 pour convertir la classe de stockage d'un objet de S3 Glacier Flexible Retrieval vers la classe de stockage S3 Glacier Deep Archive uniquement. Si vous souhaitez modifier la classe de stockage d'un objet stocké dans S3 Glacier Flexible Retrieval en une classe de stockage autre que S3 Glacier Deep Archive, vous devez d'abord utiliser l'opération de restauration pour créer une copie temporaire de l'objet. Utilisez ensuite l'opération de copie pour remplacer l'objet spécifiant S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 One Zone-IA ou Redondance réduite comme classe de stockage.
- La transition d'objets vers la classe de stockage S3 Glacier Deep Archive est unidirectionnelle.

Vous ne pouvez pas utiliser une règle de configuration du cycle de vie S3 pour convertir un objet de la classe de stockage S3 Glacier Deep Archive vers toute autre classe de stockage. Si vous souhaitez modifier la classe de stockage d'un objet archivé en une autre classe, vous devez utiliser l'opération de restauration pour effectuer d'abord une copie de l'objet. Utilisez ensuite l'opération de copie pour remplacer l'objet en spécifiant S3 Standard, S3 Intelligent-Tiering, S3 Standard-IA, S3 One Zone-IA, S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou Stockage à redondance réduite comme classe de stockage.

> **Note**
>
> L'opération de copie des objets restaurés n'est pas prise en charge dans la console Amazon S3 pour les objets des classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. Pour ce type d'opération de copie, utilisez l'API AWS Command Line Interface (AWS CLI) AWS SDKs, l'API ou l'API REST.

Les objets stockés dans les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive sont visibles et disponibles uniquement via Amazon S3. Ils ne sont pas disponibles via le service Amazon S3 Glacier séparé.

Il s'agit d'objets Amazon S3 et vous pouvez uniquement y accéder à l'aide de la console Amazon S3 ou de l'API Amazon S3. Vous ne pouvez pas accéder aux objets archivés via la console Amazon S3 Glacier séparée ou l'API Amazon S3 Glacier.

Considérations de coût

Si vous envisagez d'archiver des données rarement accédées pendant plusieurs mois ou années, les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive peuvent réduire vos coûts de stockage. Toutefois, pour vous assurer que la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive vous convient, tenez compte des éléments suivants :

- Frais généraux de stockage – Lorsque vous effectuez la transition d'objets vers la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, un volume fixe de stockage est ajouté à chaque objet pour adapter les métadonnées à la gestion de l'objet.
  - Pour chaque objet archivé dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, Amazon S3 utilise 8 Ko de stockage pour le nom de l'objet et d'autres métadonnées. Amazon S3 stocke ces métadonnées pour que vous puissiez obtenir une liste en temps réel de vos objets

archivés à l'aide de l'API Amazon S3. Pour plus d'informations, consultez Get Bucket (List Objects). Le tarif S3 Standard vous est facturé pour ce stockage supplémentaire.

- Pour chaque objet archivé dans S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive, Amazon S3 ajoute 32 Ko de stockage pour l'index et les métadonnées associées. Ces données supplémentaires sont nécessaires pour identifier et restaurer l'objet. Le tarif S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive vous est facturé pour ce stockage supplémentaire.

Si vous archivez de petits objets, tenez compte de ces frais de stockage. Pensez également à regrouper de nombreux petits objets en un plus petit nombre de gros objets afin de réduire les frais généraux.

- Nombre de jours prévu pour la conservation des objets archivés – S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive sont des solutions d'archivage à long terme. La durée minimale de stockage est de 90 jours pour la classe de stockage S3 Glacier Flexible Retrieval et de 180 jours pour S3 Glacier Deep Archive. La suppression des données archivées dans Amazon S3 Glacier n'entraîne aucuns frais si les objets que vous supprimez sont archivés depuis plus longtemps que la durée de stockage minimale. Si vous supprimez ou remplacez un objet archivé dans la durée minimale impartie, Amazon S3 facture des frais de suppression anticipés calculés au prorata. Pour plus d'informations sur les frais de suppression anticipée, consultez la question Comment les frais de suppression d'objets datant de moins de 90 jours dans Amazon S3 Glacier sont-ils facturés ? sur le FAQ sur Amazon S3.
- Frais de demande de transition S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive – Chaque objet pour lequel vous effectuez la transition vers la classe de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive constitue une demande de transition. Chaque demande de ce type a un coût. Si vous envisagez de procéder à la transition d'un grand nombre d'objets, tenez compte des coûts de demande. Si vous archivez une combinaison d'objets comprenant de petits objets, en particulier ceux de moins de 128 Ko, nous vous recommandons d'utiliser le filtre de taille d'objet du cycle de vie pour exclure les petits objets de votre transition afin de réduire les coûts liés aux demandes.
- Frais de restauration des données S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive – S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive sont conçus pour un archivage à long terme des données auxquelles vous accédez rarement. Pour plus d'informations sur les frais de restauration des données, consultez la question « Combien coûte l'extraction de données à partir d'Amazon S3 Glacier ? ». sur le FAQ sur Amazon S3. Pour plus d'informations sur la restauration des données depuis Amazon S3 Glacier, consultez Restauration d'un objet archivé.

> **Note**
>
> Le cycle de vie S3 effectue la transition des objets vers S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive de manière asynchrone. Un délai peut s'écouler entre la date de transition indiquée dans la règle de configuration de cycle de vie S3 et la date de transition physique. Dans ce cas, vous êtes facturé au tarif par défaut de la classe de stockage que vous avez quittée, sur la base de la date de transition spécifiée dans la règle.

La page détaillée du produit Amazon S3 fournit des informations sur la tarification et des exemples de calcul pour l'archivage d'objets Amazon S3. Pour plus d'informations, consultez les rubriques suivantes :

- Comment les frais de stockage pour les objets Amazon S3 archivés dans Amazon S3 Glacier sont-ils calculés ? sur le FAQ sur Amazon S3.
- Comment les frais de suppression d'objets datant de moins de 90 jours dans Amazon S3 Glacier sont-ils calculés ? sur le FAQ sur Amazon S3.
- Combien coûte l'extraction de données à partir d'Amazon S3 Glacier ? sur le FAQ sur Amazon S3.
- Tarification Amazon S3 pour les coûts de stockage concernant différentes classes de stockage.

Restauration d'objets archivés

Les objets archivés ne sont pas accessibles en temps réel. Vous devez d'abord lancer une demande de restauration puis attendre jusqu'à ce qu'une copie temporaire de l'objet soit disponible pour la durée spécifiée dans la demande. Une fois que vous avez reçu une copie temporaire de l'objet restauré, la classe de stockage de l'objet reste S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive. (Un HeadObject ou GetObjectLa demande d'opération d'API renverra S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive comme classe de stockage.)

> **Note**
>
> Lorsque vous restaurez une archive, vous payez à la fois l'archive (tarif S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive) et une copie que vous avez restaurée temporairement (tarif de stockage S3 standard). Pour obtenir des informations sur la tarification, consultez Tarification Amazon S3.

Vous pouvez restaurer la copie d'un objet par programmation ou à l'aide de la console Amazon S3. Amazon S3 ne traite qu'une seule demande de restauration simultanée par objet. Pour plus d'informations, consultez Restauration d'un objet archivé.

Objets en cours d'expiration

Vous pouvez ajouter des actions de transition à une configuration du cycle de vie S3 afin d'indiquer à Amazon S3 de supprimer les objets à la fin de leur durée de vie. Lorsqu'un objet atteint la fin de sa durée de vie selon la configuration de son cycle de vie, Amazon S3 effectue une action `Expiration` en fonction de l'état de gestion des versions S3 du compartiment :

- Compartiment sans gestion des versions : Amazon S3 met l'objet en file d'attente de suppression et le supprime de manière asynchrone, ce qui supprime définitivement l'objet.
- Compartiment activé pour la gestion des versions : si la version d'objet actuelle n'est pas un marqueur de suppression, Amazon S3 ajoute un marqueur de suppression avec un ID de version unique. Cela définit la version actuelle comme ancienne et le marqueur de suppression devient la version actuelle.
- Compartiment avec gestion des versions suspendue : Amazon S3 crée un marqueur de suppression avec l'ID de version Null. Ce marqueur de suppression remplace toute version d'objet par un ID de version nul dans la hiérarchie des versions, ce qui supprime l'objet.

Pour un compartiment avec gestion des versions (c'est-à-dire dont la gestion des versions est activée ou suspendue), plusieurs considérations guident la façon dont Amazon S3 gère l'action `Expiration`. Pour les compartiments avec gestion des versions activée ou suspendue, les règles suivantes s'appliquent :

- L'expiration d'objet s'applique uniquement à la version actuelle de l'objet (elle n'a aucun impact sur les versions d'objet non actuelles).
- Amazon S3 n'effectue aucune action en présence d'une ou de plusieurs versions d'objet et si le marqueur de suppression est la version actuelle.
- Si la version d'objet actuelle est la seule version d'objet et qu'elle est aussi un marqueur de suppression (également appelé marqueur de suppression d'objet expiré, où toutes les versions d'objet sont supprimées et où il ne reste que le marqueur de suppression), Amazon S3 supprime le marqueur de suppression d'objet expiré. Vous pouvez aussi utiliser l'action `Expiration` pour indiquer à Amazon S3 de supprimer tout marqueur de suppression d'objet expiré. Pour obtenir un exemple, consultez Suppression des marqueurs de suppression des objets expirés dans un compartiment avec gestion des versions.

- Vous pouvez utiliser l'élément d'action `NoncurrentVersionExpiration` pour indiquer à Amazon S3 de supprimer définitivement les versions non actuelles des objets. Les objets supprimés ne peuvent pas être récupérés. Vous pouvez baser cette expiration sur un certain nombre de jours depuis que les objets ne sont plus actuels. En plus du nombre de jours, vous pouvez également fournir un nombre maximal de versions non actuelles à conserver (entre 1 et 100). Cette valeur indique le nombre de nouvelles versions anciennes qui doivent exister pour qu'Amazon S3 puisse effectuer l'action associée sur une version donnée. Pour spécifier le nombre maximal de versions non actuelles, vous devez également fournir un élément `Filter`. Si vous ne spécifiez aucun élément `Filter`, Amazon S3 génère une erreur `InvalidRequest` lorsque vous fournissez un nombre maximal de versions non actuelles. Pour plus d'informations sur l'utilisation de l'élément d'action `NoncurrentVersionExpiration`, consultez the section called "Éléments pour décrire les actions du cycle de vie".
- Amazon S3 n'effectue aucune action sur les versions non actuelles des objets auxquels la configuration du verrouillage d'objet S3 est appliquée.
- Pour les objets dotés d'un statut de réplication `Pending`, Amazon S3 n'effectue aucune action sur les versions actuelles ou non actuelles des objets.

Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

> **Important**
>
> Si vous avez plusieurs règles dans une configuration du cycle de vie S3, un objet peut devenir éligible pour plusieurs actions du cycle de vie S3 le même jour. Dans de tels cas, Amazon S3 suit les règles générales suivantes :
>
> - La suppression permanente a priorité sur la transition.
> - La transition a priorité sur la création de marqueurs de suppression.
> - Si un objet est éligible pour les transitions vers S3 Glacier Flexible Retrieval et S3 Standard-IA (ou S3 One Zone-IA), Amazon S3 choisit la transition vers S3 Glacier Flexible Retrieval.
>
> Pour obtenir des exemples, consultez Exemples de chevauchement de filtres et d'actions de cycle de vie contradictoires.

Objets existants et nouveaux

Quand vous ajoutez une configuration de cycle de vie dans un compartiment, les règles de configuration s'appliquent à la fois aux objets existants et à ceux que vous ajouterez ultérieurement. À titre d'exemple, si vous ajoutez aujourd'hui une règle de configuration du cycle de vie avec une action d'expiration qui entraîne l'expiration des objets dotés d'un préfixe spécifique 30 jours après leur création, Amazon S3 met en file d'attente de suppression tous les objets de plus de 30 jours qui incluent le préfixe spécifié.

> **Important**
>
> Vous ne pouvez pas utiliser une politique de compartiment pour empêcher les suppressions ou les transitions régies par une règle de cycle de vie S3. Par exemple, même si votre politique de compartiment refuse toutes les actions pour tous les principaux, votre configuration du cycle de vie S3 continue de fonctionner normalement.

Comment savoir quand les objets vont expirer

Pour connaître la date d'expiration prévue de la version actuelle d'un objet, utilisez le HeadObject ou GetObjectFonctionnement de l'API. Ces opérations d'API renvoient des en-têtes de réponse qui indiquent la date et l'heure auxquelles la version actuelle de l'objet ne peut plus être mise en cache.

> **Note**
>
> - Un certain retard est possible entre la date d'expiration et la date à laquelle Amazon S3 supprime un objet. L'expiration de la durée de stockage associée à un objet ayant expiré n'est pas facturée.
> - Avant de mettre à jour, de désactiver ou de supprimer les règles du cycle de vie, utilisez les opérations de l'`LIST`API (telles que ListObjectsV2, ListObjectVersions, et ListMultipartUploads) ou Catalogage et analyse de vos données avec l'inventaire S3 pour vérifier qu'Amazon S3 a transféré et expiré les objets éligibles en fonction de vos cas d'utilisation.

Frais de durée minimale de stockage

Si vous créez une règle d'expiration du cycle de vie S3 entraînant l'expiration des objets appartenant aux classes de stockage S3 Standard-IA ou S3 One Zone-IA depuis moins de 30 jours, vous serez facturé pour la durée de 30 jours. Si vous créez une règle d'expiration de cycle de vie entraînant l'expiration d'objets stockés dans S3 Glacier Flexible Retrieval depuis moins de 90 jours, les 90 jours vous seront facturés. Si vous créez une règle d'expiration du cycle de vie entraînant l'expiration des objets appartenant à la classe de stockage S3 Glacier Deep Archive depuis moins de 180 jours, vous serez facturé pour la durée de 180 jours.

Pour plus d'informations, consultez Tarification Amazon S3.

Définition d'une configuration du cycle de vie S3 sur un compartiment

Vous pouvez définir une configuration du cycle de vie Amazon S3 sur un compartiment à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs Pour plus d'informations sur la configuration de cycle de vie S3, consultez Gestion du cycle de vie des objets.

> **Note**
>
> Pour consulter ou modifier la configuration du cycle de vie d'un compartiment de répertoire AWS CLI AWS SDKs, utilisez l'API REST, ou Amazon S3. Pour de plus amples informations, veuillez consulter Utilisation du cycle de vie S3 pour les compartiments de répertoires.

Dans votre configuration du cycle de vie S3, vous utilisez des règles de cycle de vie pour définir les actions que vous souhaitez qu'Amazon S3 entreprenne au cours de la durée de vie d'un objet. Par exemple, vous pouvez définir des règles pour transférer les objets vers une autre classe de stockage, archiver les objets ou les faire expirer (supprimer) après une période spécifiée.

Considérations de cycle de vie S3

Avant de définir une configuration de cycle de vie, veuillez noter ce qui suit :

Délai de propagation d'une configuration du cycle de vie

Quand vous ajoutez une configuration de cycle de vie S3 à un compartiment, il y a habituellement un certain délai avant que la nouvelle configuration de cycle de vie ou celle qui a été mise à jour ne soit

totalement appliquée à tous les systèmes Amazon S3. Il faut attendre quelques minutes avant que la configuration ne prenne effet. Ce décalage peut également se produire lors de la suppression d'une configuration de cycle de vie S3.

Délai de transition ou d'expiration

Il y a un délai entre le moment où une règle de cycle de vie est satisfaite et le moment où l'action correspondant à la règle se termine. Supposons, par exemple, qu'une règle de cycle de vie entraîne l'expiration d'un ensemble d'objets le 1er janvier. Même si la règle d'expiration a été respectée le 1er janvier, Amazon S3 ne supprimera peut-être ces objets que des jours, voire des semaines plus tard. Ce délai est dû au fait que le cycle de vie S3 met en file d'attente les objets à transférer ou à faire expirer de manière asynchrone. Toutefois, les changements de tarification sont généralement appliqués quand la règle de cycle de vie est satisfaite, même si l'action n'est pas terminée. Pour plus d'informations, consultez Changements au niveau de la facturation. Pour surveiller l'effet des mises à jour effectuées par les règles de cycle de vie actives, consultez the section called "Comment puis-je surveiller les actions prises conformément à mes règles de cycle de vie ?"

Mise à jour, désactivation ou suppression des règles de cycle de vie

Lorsque vous désactivez ou supprimez des règles de cycle de vie, Amazon S3 interrompt la planification des nouveaux objets à supprimer ou transférer après un court délai. Tous les objets déjà planifiés sont déprogrammés et ne sont ni supprimés ni transférés.

> **Note**
>
> Avant de mettre à jour, de désactiver ou de supprimer les règles du cycle de vie, utilisez les opérations `LIST` d'API (telles que ListObjectsV2, ListObjectVersions, et ListMultipartUploads) ou Catalogage et analyse de vos données avec l'inventaire S3 pour vérifier qu'Amazon S3 a transféré et expiré les objets éligibles en fonction de vos cas d'utilisation. Si vous rencontrez des problèmes lors de la mise à jour, de la désactivation ou de la suppression des règles de cycle de vie, consultez Résolution des problèmes du cycle de vie Amazon S3.

Objets existants et nouveaux

Quand vous ajoutez une configuration de cycle de vie dans un compartiment, les règles de configuration s'appliquent à la fois aux objets existants et à ceux que vous ajouterez ultérieurement. À titre d'exemple, si vous ajoutez aujourd'hui une règle de configuration du cycle de vie avec une action d'expiration qui entraîne l'expiration des objets dotés d'un préfixe spécifique 30 jours après

leur création, Amazon S3 met en file d'attente de suppression tous les objets de plus de 30 jours qui incluent le préfixe spécifié.

Surveillance de l'effet des règles de cycle de vie

Pour surveiller l'effet des mises à jour effectuées par les règles de cycle de vie actives, consultez the section called "Comment puis-je surveiller les actions prises conformément à mes règles de cycle de vie ?"

Changements au niveau de la facturation

Un délai peut s'écouler entre le moment où les règles de configuration du cycle de vie sont satisfaites et le moment où se déroule l'action déclenchée par la satisfaction de ces règles. Toutefois, des modifications de facturation interviennent dès que la règle de configuration du cycle de vie est satisfaite, même si l'action n'est pas encore entreprise.

Par exemple, après l'expiration d'un objet, son stockage ne vous est plus facturé, même si l'objet n'est pas supprimé immédiatement. De même, dès que le délai de transition d'un objet s'est écoulé, les frais de stockage S3 Glacier Flexible Retrieval vous sont facturés, même si l'objet n'est pas immédiatement transféré vers la classe de stockage S3 Glacier Flexible Retrieval.

Toutefois, les transitions du cycle de vie vers la classe de stockage S3 Intelligent-Tiering font exception. Les modifications de facturation n'interviennent qu'après le passage de l'objet dans la classe de stockage S3 Intelligent-Tiering.

Règles multiples ou contradictoires

Si vous avez plusieurs règles dans une configuration du cycle de vie S3, un objet peut devenir éligible pour plusieurs actions du cycle de vie S3 le même jour. Dans de tels cas, Amazon S3 suit les règles générales suivantes :

- La suppression permanente a priorité sur la transition.
- La transition a priorité sur la création de marqueurs de suppression.
- Si un objet est éligible pour les transitions vers S3 Glacier Flexible Retrieval et S3 Standard-IA (ou S3 One Zone-IA), Amazon S3 choisit la transition vers S3 Glacier Flexible Retrieval.

Pour obtenir des exemples, consultez Exemples de chevauchement de filtres et d'actions de cycle de vie contradictoires.

Comment définir une configuration du cycle de vie S3

Vous pouvez définir une configuration du cycle de vie Amazon S3 sur un compartiment à usage général à l'aide de la console Amazon S3, de l'API REST AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

Pour plus d'informations sur les AWS CloudFormation modèles et les exemples, voir Utilisation des AWS CloudFormation modèles et AWS::S3::Bucket dans le guide de l'utilisateur AWS CloudFormation .

Utilisation de la console S3

Vous pouvez définir des règles de cycle de vie pour tous les objets ou un sous-ensemble d'objets dans un compartiment en utilisant un préfixe partagé (noms d'objets commençant par une chaîne commune) ou une balise. Dans votre règle de cycle de vie, vous pouvez définir des actions spécifiques aux versions actuelles et non actuelles des objets. Pour plus d'informations, consultez les ressources suivantes :

- Gestion du cycle de vie des objets
- Conservation de plusieurs versions d'objets grâce à la gestion des versions S3

Pour créer une stratégie de cycle de vie

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez créer une règle de cycle de vie.
4. Choisissez l'onglet Management (Gestion), puis choisissez Create lifecycle rule (Créer une règle de cycle de vie).
5. Dans Lifecycle rule name (Nom de la règle du cycle de vie), saisissez un nom pour votre règle.

   Ce nom doit être unique dans le compartiment.
6. Choisissez l'étendue de la règle de cycle de vie :

   - Pour appliquer cette règle de cycle de vie à tous les objets avec un préfixe ou une balise spécifique, choisissez Limiter la portée à des préfixes ou balises spécifiques.

- Pour limiter l'étendue par préfixe, saisissez le préfixe dans Prefix (Préfixe).
- Pour limiter l'étendue par balise, choisissez Add tag (Ajouter une balise), puis saisissez la clé et la valeur de la balise.

Pour en savoir plus sur les préfixes de nom d'objet, consultez Attribution d'un nom aux objets Amazon S3. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.

- Pour appliquer cette règle de cycle de vie à tous les objets du compartiment, choisissez Cette règle s'applique à tous les objets du compartiment, puis Je reconnais que cette règle s'applique à tous les objets du compartiment.

7. Pour filtrer une règle par taille d'objet, vous pouvez sélectionner Spécifier la taille minimale d'objet, Spécifier la taille maximale d'objet ou les deux options.

   - Lorsque vous spécifiez une valeur pour Taille minimale d'objet ou Taille maximale d'objet, la valeur doit être comprise entre 0 octet et 5 To. Vous pouvez spécifier cette valeur en octets, Ko, Mo ou Go.
   - Si vous spécifiez les deux valeurs, la taille maximale d'objet doit être supérieure à la taille minimale d'objet.

   > **Note**
   >
   > Les filtres Taille minimale d'objet et Taille maximale d'objet excluent les valeurs spécifiées. Par exemple, si vous définissez un filtre pour faire expirer les objets ayant une Taille minimale d'objet de 128 Ko, les objets dont la taille est exactement de 128 Ko n'expirent pas. À la place, la règle s'applique uniquement aux objets d'une talle supérieure à 128 Ko.

8. Sous Lifecycle rule actions (Actions de règle de cycle de vie), choisissez les actions que votre règle de cycle de vie doit effectuer :

   - Transition current versions of objects between storage classes (Transition des versions actuelles des objets entre les classes de stockage)
   - Transition previous versions of objects between storage classes (Transition des versions précédentes des objets entre les classes de stockage)
   - Expire current versions of objects (Faire expirer les versions actuelles des objets)

> **Note**
>
> Pour les compartiments pour lesquels l'option Gestion des versions S3 n'est pas activée, l'expiration des versions actuelles entraîne la suppression définitive des objets par Amazon S3. Pour de plus amples informations, veuillez consulter the section called "Actions du cycle de vie et état de la gestion des versions du compartiment".

- Permanently delete previous versions of objects (Supprimer définitivement les versions précédentes des objets)
- Delete expired delete markers or incomplete multipart uploads (Supprimer les marqueurs de suppression expirés ou les chargements partitionnés non terminés)

Selon les actions que vous choisissez, différentes options apparaissent.

9. Pour transférer les versions actuelles des objets entre les classes de stockage, sous Transition des versions actuelles des objets entre les classes de stockage, procédez comme suit :

   a. Dans Transitions des classes de stockage, choisissez la classe de stockage vers laquelle effectuer la transition. Pour obtenir la liste des transitions possibles, consultez the section called "Transitions de cycle de vie prises en charge". Vous pouvez choisir parmi les classes de stockage suivantes :

      - S3 standard – Accès peu fréquent
      - S3 Intelligent-Tiering
      - S3 One Zone-IA
      - S3 Glacier Instant Retrieval
      - S3 Glacier Flexible Retrieval
      - S3 Glacier Deep Archive

   b. Dans Days after object creation (Jours après la création de l'objet), entrez le nombre de jours après la création pour la transition de l'objet.

   Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3. Vous pouvez définir le transfert des versions actuelles ou précédentes des objets, ou des deux versions à la fois. La gestion des versions vous

permet de conserver plusieurs versions d'un objet au sein d'un même compartiment. Pour plus d'informations sur la gestion des versions, consultez Utilisation de la console S3.

> **Important**
>
> Lorsque vous choisissez la classe de stockage S3 Glacier Instant Retrieval, S3 Glacier Flexible Retrieval ou Glacier Deep Archive, vos objets restent dans Amazon S3. Vous ne pouvez pas y accéder directement via le service Amazon S3 Glacier distinct. Pour de plus amples informations, veuillez consulter Transition des objets à l'aide du cycle de vie Amazon S3.

10. Pour transférer les versions non actuelles des objets entre les classes de stockage, sous Transition des versions non actuelles des objets entre les classes de stockage, procédez comme suit :

    a. Dans Transitions des classes de stockage, choisissez la classe de stockage vers laquelle effectuer la transition. Pour obtenir la liste des transitions possibles, consultez the section called "Transitions de cycle de vie prises en charge". Vous pouvez choisir parmi les classes de stockage suivantes :

       - S3 standard – Accès peu fréquent
       - S3 Intelligent-Tiering
       - S3 One Zone-IA
       - S3 Glacier Instant Retrieval
       - S3 Glacier Flexible Retrieval
       - S3 Glacier Deep Archive

    b. Dans Jours après lesquels les objets deviennent anciens, entrez le nombre de jours après la création pour effectuer la transition de l'objet.

11. Pour faire expirer les versions actuelles des objets, sous Expire current versions of objects (Faire expirer des versions actuelles des objets), dans Number of days after object creation (Nombre de jours après la création de l'objet), entrez le nombre de jours.

> **Important**
>
> Dans un compartiment sans gestion des versions, l'action d'expiration a pour résultat la suppression permanente de l'objet par Amazon S3. Pour en savoir plus sur les actions de cycle de vie, consultez Éléments pour décrire les actions du cycle de vie.

12. Pour supprimer définitivement les versions précédentes d'objets, sous Permanently delete noncurrent versions of objects (Supprimer définitivement les versions précédentes des objets), dans Days after objects become previous versions (Jours après que les objets deviennent des versions précédentes), entrez le nombre de jours. Vous pouvez éventuellement spécifier le nombre de versions plus récentes à conserver en saisissant une valeur sous Number of newer versions to retain (Nombre de versions plus récentes à conserver).
13. Sous Delete expired delete markers or incomplete multipart uploads (Supprimer les marqueurs de suppression expirés ou les chargements en plusieurs parties incomplets), choisissez Delete expired object delete markers (Supprimer les marqueurs de suppression d'objet arrivés à expiration) et Delete incomplete multipart uploads (Supprimer les chargements partitionnés non terminés). Entrez ensuite le nombre de jours après le début du chargement partitionné que vous souhaitez arrêter et nettoyez les chargements en plusieurs parties incomplets.

    Pour en savoir plus sur les chargements partitionnés, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.
14. Choisissez Créer une règle.

    Si la règle ne contient aucune erreur, Amazon S3 l'active et vous pouvez la voir dans l'onglet Management (Gestion) sous Lifecycle rules (Règles de cycle de vie).

À l'aide du AWS CLI

Vous pouvez utiliser les AWS CLI commandes suivantes pour gérer les configurations du cycle de vie S3 :

- `put-bucket-lifecycle-configuration`
- `get-bucket-lifecycle-configuration`
- `delete-bucket-lifecycle`

Pour obtenir des instructions sur la configuration du AWS CLI, consultez la section Développement avec Amazon S3 à l'aide de la AWS CLI dans le manuel Amazon S3 API Reference.

Notez que la configuration de cycle de vie Amazon S3 est un fichier XML. Mais lorsque vous utilisez le AWS CLI, vous ne pouvez pas spécifier le format XML. Vous devez spécifier le format JSON à la place. Vous trouverez ci-dessous des exemples de configurations de cycle de vie XML et les configurations JSON équivalentes que vous pouvez spécifier dans une AWS CLI commande.

Prenez l'exemple suivant de configuration de cycle de vie S3.

Example Exemple 1

Example

XML

```
<LifecycleConfiguration>
    <Rule>
        <ID>ExampleRule</ID>
        <Filter>
           <Prefix>documents/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "Filter": {
                "Prefix": "documents/"
            },
            "Status": "Enabled",
```

```
            "Transitions": [
                {
                    "Days": 365,
                    "StorageClass": "GLACIER"
                }
            ],
            "Expiration": {
                "Days": 3650
            },
            "ID": "ExampleRule"
        }
    ]
}
```

Example Exemple 2

Example

XML

```
<LifecycleConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <Rule>
        <ID>id-1</ID>
        <Expiration>
            <Days>1</Days>
        </Expiration>
        <Filter>
            <And>
                <Prefix>myprefix</Prefix>
                <Tag>
                    <Key>mytagkey1</Key>
                    <Value>mytagvalue1</Value>
                </Tag>
                <Tag>
                    <Key>mytagkey2</Key>
                    <Value>mytagvalue2</Value>
                </Tag>
            </And>
        </Filter>
        <Status>Enabled</Status>
    </Rule>
</LifecycleConfiguration>
```

JSON

```
{
    "Rules": [
        {
            "ID": "id-1",
            "Filter": {
                "And": {
                    "Prefix": "myprefix",
                    "Tags": [
                        {
                            "Value": "mytagvalue1",
                            "Key": "mytagkey1"
                        },
                        {
                            "Value": "mytagvalue2",
                            "Key": "mytagkey2"
                        }
                    ]
                }
            },
            "Status": "Enabled",
            "Expiration": {
                "Days": 1
            }
        }
    ]
}
```

Vous pouvez tester la commande `put-bucket-lifecycle-configuration` comme suit.

Tester la configuration

1. Enregistrez la configuration du cycle de vie au format JSON dans un fichier (par exemple, *`lifecycle.json`*).
2. Exécutez la AWS CLI commande suivante pour définir la configuration du cycle de vie de votre bucket. Remplacez *`user input placeholders`* par vos propres informations.

```
$ aws s3api put-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket  \
--lifecycle-configuration file://lifecycle.json
```

3. Pour vérifier, récupérez la configuration du cycle de vie S3 à l'aide de la `get-bucket-lifecycle-configuration` AWS CLI commande suivante :

```
$ aws s3api get-bucket-lifecycle-configuration  \
--bucket amzn-s3-demo-bucket
```

4. Pour supprimer la configuration du cycle de vie S3, utilisez la `delete-bucket-lifecycle` AWS CLI commande suivante :

```
aws s3api delete-bucket-lifecycle \
--bucket amzn-s3-demo-bucket
```

À l'aide du AWS SDKs

Java

Vous pouvez utiliser le AWS SDK pour Java pour gérer la configuration du cycle de vie S3 d'un compartiment. Pour plus d'informations sur la gestion de la configuration du cycle de vie S3, consultez Gestion du cycle de vie des objets.

> **Note**
>
> Quand vous ajoutez une configuration du cycle de vie S3 à un compartiment, Amazon S3 remplace la configuration du cycle de vie actuelle du compartiment, s'il en existe une. Pour mettre à jour une configuration, vous devez la récupérer, effectuer les modifications souhaitées, puis ajouter la configuration révisée dans le compartiment.

L'exemple suivant montre comment utiliser le pour ajouter, mettre AWS SDK pour Java à jour et supprimer la configuration du cycle de vie d'un bucket. Cet exemple effectue les opérations suivantes :

- Il ajoute une configuration de cycle de vie à un compartiment.
- Il récupère la configuration de cycle de vie et la met à jour en ajoutant une autre règle.
- Il ajoute la configuration de cycle de vie modifiée au compartiment. Amazon S3 remplace la configuration existante.
- Il récupère à nouveau la configuration et vérifie que celle-ci comporte le nombre approprié de règles en affichant ce nombre.

- Il supprime la configuration de cycle de vie et vérifie que celle-ci a été supprimée en tentant de la récupérer à nouveau.

Pour obtenir les instructions pour la création et le test d'un exemple pratique, consultez Démarrer dans le Guide du développeur AWS SDK pour Java .

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration;
import com.amazonaws.services.s3.model.BucketLifecycleConfiguration.Transition;
import com.amazonaws.services.s3.model.StorageClass;
import com.amazonaws.services.s3.model.Tag;
import com.amazonaws.services.s3.model.lifecycle.LifecycleAndOperator;
import com.amazonaws.services.s3.model.lifecycle.LifecycleFilter;
import com.amazonaws.services.s3.model.lifecycle.LifecyclePrefixPredicate;
import com.amazonaws.services.s3.model.lifecycle.LifecycleTagPredicate;

import java.io.IOException;
import java.util.Arrays;

public class LifecycleConfiguration {

        public static void main(String[] args) throws IOException {
                Regions clientRegion = Regions.DEFAULT_REGION;
                String bucketName = "*** Bucket name ***";

                // Create a rule to archive objects with the "glacierobjects/"
 prefix to Glacier
                // immediately.
                BucketLifecycleConfiguration.Rule rule1 = new
 BucketLifecycleConfiguration.Rule()
                                .withId("Archive immediately rule")
                                .withFilter(new LifecycleFilter(new
 LifecyclePrefixPredicate("glacierobjects/")))
                                .addTransition(new
 Transition().withDays(0).withStorageClass(StorageClass.Glacier))
                                .withStatus(BucketLifecycleConfiguration.ENABLED);
```

```
                // Create a rule to transition objects to the Standard-Infrequent
Access storage
                // class
                // after 30 days, then to Glacier after 365 days. Amazon S3 will
delete the
                // objects after 3650 days.
                // The rule applies to all objects with the tag "archive" set to
"true".
                BucketLifecycleConfiguration.Rule rule2 = new
BucketLifecycleConfiguration.Rule()
                                .withId("Archive and then delete rule")
                                .withFilter(new LifecycleFilter(new
LifecycleTagPredicate(new Tag("archive", "true"))))
                                .addTransition(new Transition().withDays(30)

.withStorageClass(StorageClass.StandardInfrequentAccess))
                                .addTransition(new
Transition().withDays(365).withStorageClass(StorageClass.Glacier))
                                .withExpirationInDays(3650)
                                .withStatus(BucketLifecycleConfiguration.ENABLED);

                // Add the rules to a new BucketLifecycleConfiguration.
                BucketLifecycleConfiguration configuration = new
BucketLifecycleConfiguration()
                                .withRules(Arrays.asList(rule1, rule2));

                try {
                        AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                                        .withCredentials(new
ProfileCredentialsProvider())
                                        .withRegion(clientRegion)
                                        .build();

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
configuration);

                        // Retrieve the configuration.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Add a new rule with both a prefix predicate and a tag
predicate.
```

```
                        configuration.getRules().add(new
BucketLifecycleConfiguration.Rule().withId("NewRule")
                                        .withFilter(new LifecycleFilter(new
LifecycleAndOperator(
                                                                Arrays.asList(new
LifecyclePrefixPredicate("YearlyDocuments/"),
                                                                                new
LifecycleTagPredicate(new Tag(

   "expire_after",

   "ten_years"))))))
                                        .withExpirationInDays(3650)

.withStatus(BucketLifecycleConfiguration.ENABLED));

                        // Save the configuration.
                        s3Client.setBucketLifecycleConfiguration(bucketName,
configuration);

                        // Retrieve the configuration.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration now has three rules.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);
                        System.out.println("Expected # of rules = 3; found: " +
configuration.getRules().size());

                        // Delete the configuration.
                        s3Client.deleteBucketLifecycleConfiguration(bucketName);

                        // Verify that the configuration has been deleted by
attempting to retrieve it.
                        configuration =
s3Client.getBucketLifecycleConfiguration(bucketName);
                        String s = (configuration == null) ? "No configuration
found." : "Configuration found.";
                        System.out.println(s);
                } catch (AmazonServiceException e) {
                        // The call was transmitted successfully, but Amazon S3
couldn't process
                        // it, so it returned an error response.
```

```
                        e.printStackTrace();
                } catch (SdkClientException e) {
                        // Amazon S3 couldn't be contacted for a response, or the
 client
                        // couldn't parse the response from Amazon S3.
                        e.printStackTrace();
                }
        }
}
```

.NET

Vous pouvez utiliser le AWS SDK pour .NET pour gérer la configuration du cycle de vie S3 sur un bucket. Pour plus d'informations sur la gestion de la configuration du cycle de vie, consultez Gestion du cycle de vie des objets.

> **Note**
>
> Quand vous ajoutez une configuration de cycle de vie, Amazon S3 remplace la configuration existante sur le compartiment spécifié. Pour mettre à jour une configuration, vous devez d'abord récupérer la configuration de cycle de vie, effectuer les modifications, puis ajouter la configuration modifiée dans le compartiment.

L'exemple suivant montre comment utiliser le pour ajouter, mettre AWS SDK pour .NET à jour et supprimer la configuration du cycle de vie d'un bucket. L'exemple de code effectue les opérations suivantes :

- Il ajoute une configuration de cycle de vie à un compartiment.
- Il récupère la configuration de cycle de vie et la met à jour en ajoutant une autre règle.
- Il ajoute la configuration de cycle de vie modifiée au compartiment. Amazon S3 remplace la configuration de cycle de vie existante.
- Il récupère à nouveau la configuration de cycle de vie et la vérifie en affichant le nombre de règles qu'elle contient.
- Il supprime la configuration de cycle de vie et vérifie qu'elle a été supprimée.

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Premiers pas avec le kit AWS SDK pour .NET dans le Guide du développeur AWS SDK pour .NET .

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class LifecycleTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddUpdateDeleteLifecycleConfigAsync().Wait();
        }

        private static async Task AddUpdateDeleteLifecycleConfigAsync()
        {
            try
            {
                var lifeCycleConfiguration = new LifecycleConfiguration()
                {
                    Rules = new List<LifecycleRule>
                        {
                            new LifecycleRule
                            {
                                 Id = "Archive immediately rule",
                                 Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
 LifecyclePrefixPredicate()
                                     {
                                         Prefix = "glacierobjects/"
```

```
                                    }
                                },
                                Status = LifecycleRuleStatus.Enabled,
                                Transitions = new List<LifecycleTransition>
                                {
                                     new LifecycleTransition
                                     {
                                          Days = 0,
                                          StorageClass = S3StorageClass.Glacier
                                     }
                                 },
                            },
                            new LifecycleRule
                            {
                                 Id = "Archive and then delete rule",
                                  Filter = new LifecycleFilter()
                                 {
                                     LifecycleFilterPredicate = new
LifecyclePrefixPredicate()
                                     {
                                         Prefix = "projectdocs/"
                                     }
                                 },
                                 Status = LifecycleRuleStatus.Enabled,
                                 Transitions = new List<LifecycleTransition>
                                 {
                                      new LifecycleTransition
                                      {
                                           Days = 30,
                                           StorageClass =
S3StorageClass.StandardInfrequentAccess
                                      },
                                      new LifecycleTransition
                                      {
                                        Days = 365,
                                        StorageClass = S3StorageClass.Glacier
                                      }
                                 },
                                 Expiration = new LifecycleRuleExpiration()
                                 {
                                       Days = 3650
                                 }
                            }
                        }
```

```
                };

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Retrieve an existing configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

                // Add a new rule.
                lifeCycleConfiguration.Rules.Add(new LifecycleRule
                {
                    Id = "NewRule",
                    Filter = new LifecycleFilter()
                    {
                        LifecycleFilterPredicate = new LifecyclePrefixPredicate()
                        {
                            Prefix = "YearlyDocuments/"
                        }
                    },
                    Expiration = new LifecycleRuleExpiration()
                    {
                        Days = 3650
                    }
                });

                // Add the configuration to the bucket.
                await AddExampleLifecycleConfigAsync(client,
lifeCycleConfiguration);

                // Verify that there are now three rules.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);
                Console.WriteLine("Expected # of rulest=3; found:{0}",
lifeCycleConfiguration.Rules.Count);

                // Delete the configuration.
                await RemoveLifecycleConfigAsync(client);

                // Retrieve a nonexistent configuration.
                lifeCycleConfiguration = await RetrieveLifecycleConfigAsync(client);

            }
            catch (AmazonS3Exception e)
            {
```

```
                Console.WriteLine("Error encountered ***. Message:'{0}' when writing
an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task AddExampleLifecycleConfigAsync(IAmazonS3 client,
LifecycleConfiguration configuration)
        {

            PutLifecycleConfigurationRequest request = new
PutLifecycleConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };
            var response = await client.PutLifecycleConfigurationAsync(request);
        }

        static async Task<LifecycleConfiguration>
RetrieveLifecycleConfigAsync(IAmazonS3 client)
        {
            GetLifecycleConfigurationRequest request = new
GetLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            var response = await client.GetLifecycleConfigurationAsync(request);
            var configuration = response.Configuration;
            return configuration;
        }

        static async Task RemoveLifecycleConfigAsync(IAmazonS3 client)
        {
            DeleteLifecycleConfigurationRequest request = new
DeleteLifecycleConfigurationRequest
            {
                BucketName = bucketName
            };
            await client.DeleteLifecycleConfigurationAsync(request);
```

```
        }
    }
}
```

Ruby

Vous pouvez utiliser le AWS SDK pour Ruby pour gérer une configuration du cycle de vie S3 sur un compartiment en utilisant la classe AWS::S3::BucketLifecycleConfiguration. Pour plus d'informations sur la gestion de la configuration du cycle de vie S3, consultezGestion du cycle de vie des objets.

Utilisation de l'API REST

Les rubriques suivantes de la Référence d'API Amazon Simple Storage Service décrivent les opérations d'API REST associées à la configuration du cycle de vie S3 :

- PutBucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- DeleteBucketLifecycle

Résolution des problèmes liés au cycle de vie S3

Pour découvrir les problèmes courants susceptibles de se produire lors de l'utilisation du cycle de vie S3, consultez the section called "Résolution des problèmes du cycle de vie".

Comment le cycle de vie S3 interagit avec d'autres configurations de compartiments

En plus des configurations de cycle de vie S3, vous pouvez associer d'autres configurations à votre compartiment. Cette section explique comment la configuration de cycle de vie S3 est associée aux autres configurations de compartiment.

Cycle de vie S3 et gestion des versions S3

Vous pouvez ajouter des configurations de cycle de vie S3 aux compartiments sans gestion des versions et aux compartiments pour lesquels la gestion des versions d'objet est activée. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Un compartiment activé pour le contrôle de version maintient une version d'objet actuelle et aucune ou plusieurs versions d'objets anciennes. Vous pouvez définir des règles de cycle de vie séparées pour les versions d'objet actuelles et anciennes.

Pour de plus amples informations, veuillez consulter Éléments de la configuration du cycle de vie.

> **Important**
>
> Si vous avez plusieurs règles dans une configuration du cycle de vie S3, un objet peut devenir éligible pour plusieurs actions du cycle de vie S3 le même jour. Dans de tels cas, Amazon S3 suit les règles générales suivantes :
>
> - La suppression permanente a priorité sur la transition.
> - La transition a priorité sur la création de marqueurs de suppression.
> - Si un objet est éligible pour les transitions vers S3 Glacier Flexible Retrieval et S3 Standard-IA (ou S3 One Zone-IA), Amazon S3 choisit la transition vers S3 Glacier Flexible Retrieval.
>
> Pour obtenir des exemples, consultez Exemples de chevauchement de filtres et d'actions de cycle de vie contradictoires.

Configuration du cycle de vie S3 sur des compartiments avec authentification MFA

La configuration du cycle de vie S3 sur des compartiments d'authentification multifactorielle configurés pour la suppression MFA n'est pas prise en charge. Pour de plus amples informations, veuillez consulter Configuration de la fonction Supprimer MFA.

Cycle de vie S3 et journalisation

Les actions du cycle de vie Amazon S3 ne sont pas capturées par la journalisation au niveau de AWS CloudTrail l'objet. CloudTrailcapture les demandes d'API adressées aux points de terminaison Amazon S3 externes, tandis que les actions S3 Lifecycle sont effectuées à l'aide de points de terminaison Amazon S3 internes.

Vous pouvez activer les journaux d'accès au serveur Amazon S3 dans un compartiment S3 pour capturer des actions liées au cycle de vie S3, telles que les transitions d'objets vers une autre classe de stockage et les expirations d'objets qui aboutissent à une suppression permanente ou

à une suppression logique. Pour de plus amples informations, veuillez consulter the section called "Enregistrement de l'accès au serveur".

Si la journalisation est activée sur votre compartiment, les journaux d'accès au serveur Amazon S3 signalent les résultats des opérations suivantes.

Journal d'opération	Description
`S3.EXPIRE.OBJECT`	Amazon S3 supprime définitivement l'objet en raison de l'action `Expiration` du cycle de vie.
`S3.CREATE.DELETEMARKER`	Amazon S3 supprime logiquement la version actuelle en ajoutant un marqueur de suppression dans un compartiment avec gestion des versions.
`S3.TRANSITION_SIA.OBJECT`	Amazon S3 effectue la transition de l'objet vers la classe de stockage S3 standard – Accès peu fréquent.
`S3.TRANSITION_ZIA.OBJECT`	Amazon S3 effectue la transition de l'objet vers la classe de stockage S3 One Zone-IA.
`S3.TRANSITION_INT.OBJECT`	Amazon S3 effectue la transition de l'objet vers la classe de stockage S3 Intelligent-Tiering.
`S3.TRANSITION_GIR.OBJECT`	Amazon S3 déclenche la transition de l'objet vers la classe de stockage S3 Glacier Instant Retrieval.
`S3.TRANSITION.OBJECT`	Amazon S3 déclenche la transition de l'objet vers la classe de stockage S3 Glacier Flexible Retrieval.
`S3.TRANSITION_GDA.OBJECT`	Amazon S3 déclenche la transition de l'objet vers la classe de stockage S3 Glacier Deep Archive.

Journal d'opération	Description
`S3.DELETE.UPLOAD`	Amazon S3 abandonne un chargement partitionné incomplet.

> **Note**
>
> Les enregistrements des journaux d'accès au serveur Amazon S3 sont fournis sur la base du meilleur effort et ne peuvent pas être utilisés pour une comptabilisation complète de toutes les demandes Amazon S3.

Configuration des notifications d'événements du cycle de vie S3

Pour être averti quand Amazon S3 supprime un objet ou le transfère vers une autre classe de stockage Amazon S3 à la suite de l'application d'une règle du cycle de vie S3, vous pouvez configurer une notification d'événement Amazon S3.

Vous pouvez recevoir des notifications pour les événements du cycle de vie S3 suivants :

- Événements de transition : en utilisant le type d'événement `s3:LifecycleTransition`, vous pouvez recevoir une notification quand un objet est transféré d'une classe de stockage Amazon S3 à une autre par une configuration du cycle de vie S3.
- Événements d'expiration (suppression) : en utilisant les types d'événements `LifecycleExpiration`, vous pouvez recevoir des notifications chaque fois qu'Amazon S3 supprime un objet en fonction de votre configuration du cycle de vie S3.

  Il existe deux types d'événements d'expiration :

  - Le type d'événement `s3:LifecycleExpiration:Delete` vous avertit lorsqu'un objet figurant dans un compartiment sans gestion des versions est supprimé. `s3:LifecycleExpiration:Delete` vous avertit également lorsqu'une version d'objet est définitivement supprimée par une configuration du cycle de vie S3.
  - Le type d'événement `s3:LifecycleExpiration:DeleteMarkerCreated` vous avertit lorsque le cycle de vie S3 crée un marqueur de suppression après la suppression d'une version actuelle d'un objet dans un compartiment avec gestion des versions. S3 Lifecycle définit l'heure de création du marqueur de suppression à 00:00 UTC (minuit) du jour en cours. Cette heure de création peut être différente de l'heure de l'événement indiquée dans

la `s3:LifecycleExpiration:DeleteMarkerCreated` notification envoyée par S3. Pour de plus amples informations, veuillez consulter the section called "Suppression des versions d'objet".

Amazon S3 peut publier des notifications d'événements sur une rubrique Amazon Simple Notification Service (Amazon SNS), une file d'attente Amazon Simple Queue Service (Amazon SQS) ou une fonction. AWS Lambda Pour de plus amples informations, veuillez consulter Notifications d'événements Amazon S3.

Pour savoir comment configurer les notifications d'événements Amazon S3, consultez Activation des notifications d'événements à l'aide d'Amazon SQS, Amazon SNS et. AWS Lambda

Le message suivant est un exemple de message envoyé par Amazon S3 pour publier un événement `s3:LifecycleExpiration:Delete`. Pour de plus amples informations, veuillez consulter the section called "Structure des messages d'événements".

```
{
   "Records":[
      {
         "eventVersion":"2.3",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"LifecycleExpiration:Delete",
         "userIdentity":{
            "principalId":"s3.amazonaws.com"
         },
         "requestParameters":{
            "sourceIPAddress":"s3.amazonaws.com"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
```

```
                "principalId":"A3NL1KOZZKExample"
             },
             "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
          },
          "object":{
             "key":"expiration/delete",
             "sequencer":"0055AED6DCD90281E5",
          }
       }
    }
 ]
}
```

Les messages qu'Amazon S3 envoie pour publier un événement `s3:LifecycleTransition` comprennent également les informations suivantes :

```
"lifecycleEventData":{
    "transitionEventData": {
        "destinationStorageClass": the destination storage class for the object
    }
}
```

Éléments de la configuration du cycle de vie

Une configuration du cycle de vie S3 comprend des règles de cycle de vie qui incluent divers éléments décrivant les actions qu'Amazon S3 entreprend pendant la durée de vie des objets. Vous spécifiez une configuration du cycle de vie Amazon S3 au format XML, composée d'une ou de plusieurs règles de cycle de vie, chaque règle étant constituée d'un ou de plusieurs éléments.

```
<LifecycleConfiguration>
    <Rule>
         <Element>
    </Rule>
    <Rule>
         <Element>
         <Element>
    </Rule>
</LifecycleConfiguration>
```

Chaque règle se compose des éléments suivants :

- Des métadonnées de règle comprenant un ID de règle et un statut indiquant si la règle est activée ou non. Si une règle est désactivée, Amazon S3 n'exécute aucune action spécifiée dans la règle.
- Un filtre qui identifie les objets auxquels la règle s'applique. Vous pouvez spécifier un filtre en utilisant la taille de l'objet, le préfixe de clé d'objet, une ou plusieurs balises d'objet, ou une combinaison de filtres.
- Une ou plusieurs actions de transition ou d'expiration avec une date ou une durée dans le cycle de vie de l'objet lorsque vous voulez qu'Amazon S3 exécute l'action spécifiée.

Rubriques

- Élément d'ID
- Élément de statut
- Élément de filtre
- Éléments pour décrire les actions du cycle de vie
- Ajout de filtres à des règles de cycle de vie

Les sections suivantes décrivent les éléments XML dans une configuration de cycle de vie S3. Pour obtenir des exemples de configuration, consultez Exemples de configurations du cycle de vie S3.

Élément d'ID

Une configuration de cycle de vie S3 peut contenir jusqu'à 1 000 règles. Cette limite n'est pas réglable. L'élément `<ID>` identifie une règle de manière unique. La longueur des ID est limitée à 255 caractères.

Élément de statut

La valeur de l'élément `<Status>` peut être `Enabled` ou `Disabled`. Si une règle est désactivée, Amazon S3 n'exécute aucune action définie dans la règle.

Élément de filtre

Une règle de cycle de vie S3 peut s'appliquer à l'ensemble ou à un sous-ensemble des objets dans un compartiment en fonction de l'élément `<Filter>` que vous spécifiez dans la règle.

Vous pouvez filtrer les objets par préfixe de clé, balises d'objet ou une combinaison des deux (auquel cas, Amazon S3 utilise un opérateur logique `AND` pour combiner les filtres). Pour des exemples et plus d'informations sur les filtres, consultez Ajout de filtres à des règles de cycle de vie.

- Spécification d'un filtre à l'aide de préfixes de clé : cet exemple montre une règle de cycle de vie S3 qui s'applique à un sous-ensemble d'objets en fonction du préfixe du nom de clé (`logs/`). Par exemple, la règle de cycle de vie s'applique aux objets `logs/mylog.txt`, `logs/temp1.txt` et `logs/test.txt`. La règle ne s'applique pas à l'objet `example.jpg`.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

Si vous souhaitez appliquer une action de cycle de vie à un sous-ensemble d'objets en fonction de préfixes de noms de clé différents, spécifiez des règles distinctes. Dans chaque règle, spécifiez un filtre basé sur le préfixe. Par exemple, pour décrire une action de cycle de vie pour les objets avec les préfixes de clé `projectA/` et `projectB/`, vous spécifiez deux règles comme suit :

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>
</LifecycleConfiguration>
```

Pour en savoir plus sur les clés d'objet, consultez Attribution d'un nom aux objets Amazon S3.

- Spécification d'un filtre en fonction de balises d'objet : dans l'exemple suivant, la règle de cycle de vie spécifie un filtre basé sur une balise (*key*) et une valeur (*value*). La règle s'applique ensuite uniquement à un sous-ensemble d'objets avec la balise spécifique.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
           </Tag>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

Vous pouvez spécifier un filtre basé sur plusieurs balises. Vous devez encapsuler les balises dans l'élément <And>, comme illustré dans l'exemple suivant. La règle indique à Amazon S3 d'exécuter des actions de cycle de vie sur des objets avec deux balises (avec la clé de balise et la valeur spécifiques).

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
          </And>
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

La règle de cycle de vie s'applique aux objets qui ont tous deux des balises spécifiées. Amazon S3 effectue une opération logique AND. Remarques :

- Chaque balise doit correspondre exactement à la fois à la clé et à la valeur. Si vous spécifiez uniquement un élément <Key> et aucun élément <Value>, la règle ne s'applique qu'aux objets correspondant à la clé de balise et pour lesquels aucune valeur n'est spécifiée.
- La règle s'applique à un sous-ensemble d'objets dont toutes les étiquettes sont spécifiées dans la règle. Si un objet dispose d'étiquettes supplémentaires spécifiées, la règle continue à s'appliquer.

> **Note**
>
> Lorsque vous spécifiez plusieurs balises dans un filtre, chaque clé de balise doit être unique.

- Spécification d'un filtre basé à la fois sur le préfixe et sur une ou plusieurs balises : dans une règle de cycle de vie, vous pouvez spécifier un filtre basé à la fois sur le préfixe de clé et sur une ou plusieurs balises. Là encore, vous devez encapsuler tous ces éléments de filtre dans l'élément <And>, comme suit :

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
          <And>
             <Prefix>key-prefix</Prefix>
             <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
             </Tag>
             <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
             </Tag>
              ...
          </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Amazon S3 associe ces filtres à l'aide d'un opérateur logique AND. Autrement dit, la règle s'applique au sous-ensemble des objets dotés du préfixe de clé spécifié et des balises spécifiées. Un filtre peut avoir seulement un préfixe et zéro, une ou plusieurs balises.

- Vous pouvez spécifier un filtre vide, auquel cas la règle s'applique à tous les objets dans le compartiment.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- Pour filtrer une règle par taille d'objet, vous pouvez spécifier une taille minimale (`ObjectSizeGreaterThan`) ou une taille maximale (`ObjectSizeLessThan`), ou vous pouvez spécifier une plage de tailles d'objet.

  Les valeurs de taille d'objet sont exprimées en octets. Par défaut, les objets de moins de 128 Ko ne seront transférés vers aucune classe de stockage, sauf si vous spécifiez une taille minimale (`ObjectSizeGreaterThan`) inférieure ou une taille maximale (`ObjectSizeLessThan`). Pour de plus amples informations, veuillez consulter Exemple : permettre la transition d'objets de moins de 128 Ko.

```
                <LifecycleConfiguration>
    <Rule>
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> Les filtres `ObjectSizeGreaterThan` et `ObjectSizeLessThan` excluent les valeurs spécifiées. Par exemple, si vous définissez que les objets d'une taille comprise entre 128 Ko et 1 024 Ko doivent passer de la classe de stockage S3 Standard à la classe de stockage S3 Standard-IA, les objets qui font exactement 1 024 Ko ou 128 Ko ne passeront pas à S3 Standard-IA. À la place, la règle s'appliquera uniquement aux objets de plus de 128 Ko et de moins de 1 024 Ko.

Si vous spécifiez une plage de tailles d'objet, l'entier `ObjectSizeGreaterThan` doit être inférieur à la valeur `ObjectSizeLessThan`. Si vous utilisez plusieurs filtres, vous devez les envelopper dans un élément <And>. L'exemple suivant montre comment spécifier des objets dans une plage comprise entre 500 et 64 000 octets.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Éléments pour décrire les actions du cycle de vie

Vous pouvez indiquer à Amazon S3 d'exécuter des actions spécifiques dans le cycle de vie d'un objet en spécifiant une ou plusieurs des actions prédéfinies dans une règle de cycle de vie S3. L'effet de ces actions dépend de l'état de la gestion des versions de votre compartiment.

- Élément d'action **`Transition`** : vous spécifiez l'action `Transition` pour transférer les objets d'une classe de stockage vers une autre. Pour en savoir plus sur la transition d'objets, consultez

Transitions prises en charge. Lorsqu'une date ou une durée spécifiée dans le cycle de vie d'un objet est atteinte, Amazon S3 effectue la transition.

Pour un compartiment avec gestion des versions (compartiment activé pour la gestion des versions ou suspendu pour la gestion des versions), l'action `Transition` s'applique à la version d'objet actuelle. Pour gérer des versions anciennes, Amazon S3 définit l'action `NoncurrentVersionTransition` (décrite ultérieurement dans cette rubrique).

- Élément d'action **`Expiration`** : l'action `Expiration` fait expirer les objets identifiés dans la règle et s'applique aux objets éligibles dans l'une des classes de stockage Amazon S3. Pour plus d'informations sur les classes de stockage, consultez Bien comprendre et gérer les classes de stockage Amazon S3. Amazon S3 rend tous les objets expirés indisponibles. Que les objets soient supprimés définitivement ou pas dépend de l'état de la gestion des versions du compartiment.
  - Compartiment sans gestion des versions : l'action `Expiration` entraîne la suppression définitive de l'objet par Amazon S3.
  - Compartiment activé pour la gestion des versions – Pour un compartiment activé pour la gestion des versions (c'est-à-dire dont la gestion des versions est activée ou désactivée), plusieurs considérations guident la façon dont Amazon S3 gère l'action `Expiration`. Pour les compartiments avec gestion des versions activée ou suspendue, les règles suivantes s'appliquent :
    - L'action `Expiration` s'applique uniquement à la version actuelle (elle n'a aucun impact sur les versions d'objet anciennes).
    - Amazon S3 n'effectue aucune action en présence d'une ou de plusieurs versions d'objet et si le marqueur de suppression est la version actuelle.
    - Si la version d'objet actuelle est la seule version d'objet et qu'elle est aussi un marqueur de suppression (également appelé marqueur de suppression d'objet expiré, où toutes les versions d'objet sont supprimées et où il ne reste que le marqueur de suppression), Amazon S3 supprime le marqueur de suppression d'objet expiré. Vous pouvez aussi utiliser l'action d'expiration pour indiquer à Amazon S3 de supprimer tout marqueur de suppression d'objet expiré. Pour obtenir un exemple, consultez Suppression des marqueurs de suppression des objets expirés dans un compartiment avec gestion des versions.

    Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Tenez également compte de ce qui suit lors de la configuration d'Amazon S3 pour gérer l'expiration :

- Compartiment activé pour la gestion des versions

  Si la version d'objet actuelle n'est pas un marqueur de suppression, Amazon S3 ajoute un marqueur de suppression avec un ID de version unique. Cela définit la version actuelle comme ancienne et le marqueur de suppression devient la version actuelle.

- Compartiment suspendu pour la gestion des versions

  Dans un compartiment où la gestion des versions est suspendue, l'action d'expiration entraîne la création par Amazon S3 d'un marqueur de suppression avec l'ID de version `null`. Ce marqueur de suppression remplace toute version d'objet par un ID de version nul dans la hiérarchie des versions, ce qui supprime l'objet.

De plus, Amazon S3 fournit les actions suivantes que vous pouvez utiliser pour gérer des versions d'objet anciennes dans un compartiment activé pour la gestion des versions (c'est-à-dire, un compartiment dont la gestion des versions est activée ou désactivée).

- Élément d'action **`NoncurrentVersionTransition`** : utilisez cette action pour spécifier quand Amazon S3 doit transférer des objets vers la classe de stockage spécifiée. Vous pouvez baser cette transition sur le nombre de jours écoulés depuis que les objets sont devenus non courants (`<NoncurrentDays>`). Outre le nombre de jours, vous pouvez également spécifier le nombre de versions non actuelles (`<NewerNoncurrentVersions>`) à conserver (entre 1 et 100). Cette valeur détermine le nombre de nouvelles versions non actuelles qui doivent exister avant qu'Amazon S3 puisse effectuer la transition vers une version donnée. Amazon S3 transférera toutes les versions non actuelles supplémentaires au-delà du nombre spécifié à conserver. Pour que la transition se produise, les valeurs `<NoncurrentDays>` et les `<NewerNoncurrentVersions>` valeurs doivent être dépassées.

  Pour spécifier le nombre de versions non actuelles à conserver, vous devez également fournir un `<Filter>` élément. Si vous ne spécifiez aucun `<Filter>` élément, Amazon S3 génère une `InvalidRequest` erreur lorsque vous spécifiez le nombre de versions non actuelles à conserver.

  Pour en savoir plus sur la transition d'objets, consultez Transitions prises en charge. Pour plus de détails sur la façon dont Amazon S3 calcule la date lorsque vous spécifiez le nombre de jours dans l'action `NoncurrentVersionTransition`, consultez Règles de cycle de vie : en fonction de l'âge de l'objet.

- Élément d'action **`NoncurrentVersionExpiration`** : utilisez cette action pour indiquer à Amazon S3 de supprimer définitivement les versions non actuelles des objets. Les objets supprimés ne peuvent pas être récupérés. Vous pouvez baser cette expiration sur un certain nombre de jours depuis que les objets sont devenus caducs (`<NoncurrentDays>`). Outre le nombre de jours, vous pouvez également spécifier le nombre de versions non actuelles (`<NewerNoncurrentVersions>`) à conserver (entre 1 et 100). Cette valeur indique le nombre de nouvelles versions non actuelles qui doivent exister avant qu'Amazon S3 puisse expirer une version donnée. Amazon S3 supprime définitivement toutes les versions non actuelles supplémentaires au-delà du nombre spécifié à conserver. Pour que la suppression ait lieu, les valeurs `<NoncurrentDays>` et les `<NewerNoncurrentVersions>` valeurs doivent être dépassées.

  Pour spécifier le nombre de versions non actuelles à conserver, vous devez également fournir un `<Filter>` élément. Si vous ne spécifiez aucun `<Filter>` élément, Amazon S3 génère une `InvalidRequest` erreur lorsque vous spécifiez le nombre de versions non actuelles à conserver.

  La suppression retardée d'objets anciens peut être utile lorsque vous avez besoin de corriger des suppressions ou des remplacements accidentels. Par exemple, vous pouvez configurer une règle d'expiration pour supprimer les versions anciennes cinq jours après qu'elles soient devenues anciennes. Par exemple, supposons que le 01/01/2014, à 10 h 30 UTC, vous créez un objet appelé `photo.gif` (ID de version 111111). Le 02/01/2014 à 11 h 30 UTC, vous supprimez par inadvertance `photo.gif` (ID de version 111111), ce qui crée un marqueur de suppression avec un nouvel ID de version (tel que l'ID de version 4857693). Vous avez à présent cinq jours pour récupérer la version d'origine de `photo.gif` (ID de version 111111) avant que la suppression ne soit définitive. Le 08/01/2014 à 00 h 00 UTC, la règle de cycle de vie pour l'expiration s'exécute et supprime définitivement `photo.gif` (ID de version 111111), cinq jours après qu'il est devenu une version non actuelle.

  Pour plus de détails sur la façon dont Amazon S3 calcule la date lorsque vous spécifiez le nombre de jours dans une action `NoncurrentVersionExpiration`, consultez Règles de cycle de vie : en fonction de l'âge de l'objet.

  > **Note**
  >
  > Les configurations de cycle de vie de l'expiration d'objet ne suppriment pas les chargements partitionnés incomplets. Pour supprimer les chargements

partitionnés incomplets, vous devez utiliser l'action de configuration du cycle de vie `AbortIncompleteMultipartUpload`, décrite plus loin dans cette section.

En plus des actions de transition et d'expiration, vous pouvez utiliser les actions de configuration du cycle de vie suivantes pour indiquer à Amazon S3 d'arrêter les chargements partitionnés incomplets ou de supprimer les marqueurs de suppression des objets expirés.

- Élément d'action **`AbortIncompleteMultipartUpload`** : utilisez cet élément pour définir une durée maximale (en jours) pendant laquelle vous souhaitez autoriser la poursuite des chargements partitionnés. Si les chargements partitionnés applicables (déterminés par le nom de clé `prefix` spécifié dans la règle de cycle de vie) ne sont pas correctement menés à terme dans la période prédéfinie, Amazon S3 arrête les chargements partitionnés incomplets. Pour de plus amples informations, veuillez consulter Interruption d'un chargement partitionné.

  > **Note**
  >
  > Vous ne pouvez pas spécifier cette action de cycle de vie dans une règle dotée d'un filtre utilisant des balises d'objet.

- Élément d'action **`ExpiredObjectDeleteMarker`** : dans un compartiment avec gestion des versions, un marqueur de suppression sans aucune version non actuelle est désigné en tant que marqueur de suppression d'objet expiré. Vous pouvez utiliser cette action de cycle de vie pour indiquer à Amazon S3 de supprimer les marqueurs de suppression d'objets expirés. Pour obtenir un exemple, consultez Suppression des marqueurs de suppression des objets expirés dans un compartiment avec gestion des versions.

  > **Note**
  >
  > Vous ne pouvez pas spécifier cette action de cycle de vie dans une règle dotée d'un filtre utilisant des balises d'objet.

Comment Amazon S3 calcule le temps depuis lequel un objet est ancien

Un compartiment sur lequel la gestion des versions est activée peut contenir de nombreuses versions d'un objet. Il y a toujours une version actuelle et éventuellement une ou plusieurs versions anciennes. Chaque fois que vous chargez un objet, la version actuelle est retenue comme version ancienne

et la version nouvellement ajoutée, le successeur, devient la version actuelle. Pour déterminer le nombre de jours depuis lequel un objet est ancien, Amazon S3 regarde la date de création de son successeur. Amazon S3 utilise le nombre de jours depuis la création de son successeur comme le nombre de jours depuis lequel un objet est ancien.

Restauration des versions précédentes d'un objet lorsque les configurations de cycle de vie S3 sont utilisées

Comme cela est expliqué dans Restauration des versions précédentes, vous pouvez utiliser l'une des deux méthodes suivantes pour récupérer des versions précédentes d'un objet :

- Méthode 1 : copier une version non actuelle de l'objet dans le même compartiment. L'objet copié devient la version actuelle de cet objet et toutes les versions d'objet sont préservées.
- Méthode 2 : supprimer définitivement la version actuelle de l'objet. Lorsque vous supprimez la version d'objet actuelle, vous transformez la version ancienne en version actuelle de cet objet.

Lorsque vous utilisez des règles de configuration du cycle de vie S3 avec des compartiments avec gestion des versions, nous recommandons comme bonne pratique d'utiliser la méthode 1.
Le cycle de vie S3 fonctionne sous un modèle éventuellement cohérent. Une version actuelle que vous avez supprimée définitivement peut ne pas disparaître tant que les changements n'ont pas été propagés à tous les systèmes Amazon S3. (Par conséquent, Amazon S3 n'est peut-être temporairement pas conscient de cette suppression.) Entre temps, la règle de cycle de vie que vous avez configurée pour l'expiration des objets anciens peut supprimer définitivement des objets anciens, y compris celui que vous souhaitez restaurer. Par conséquent, la copie de l'ancienne version, telle que recommandée dans la méthode 1, constitue l'alternative la plus sûre.

Actions du cycle de vie et état de la gestion des versions du compartiment

Règles de cycle de vie : en fonction de l'âge de l'objet

Vous pouvez spécifier un délai, en nombre de jours à compter de la création (ou de la modification) de l'objet, pendant lequel Amazon S3 peut entreprendre l'action spécifiée.

Lorsque vous spécifiez le nombre de jours dans les actions `Transition` et `Expiration` dans une configuration de cycle de vie S3, notez ce qui suit :

- La valeur que vous spécifiez correspond au nombre de jours écoulés depuis la création de l'objet au cours desquels l'action se produira.
- Amazon S3 calcule l'heure en ajoutant le nombre de jours spécifié dans la règle à l'heure de création de l'objet et en arrondissant le temps obtenu au jour suivant à minuit UTC. Par exemple, si un objet a été créé le 15/01/2014 à 10 h 30 UTC et que vous spécifiez 3 jours dans une règle de transition, la date calculée de transition de l'objet sera le 19/01/2014 à 00 h 00 UTC.

> **Note**
>
> Amazon S3 conserve uniquement la dernière date de modification pour chaque objet. Par exemple, la console Amazon S3 affiche la date Dernière modification dans le volet Propriétés de l'objet. Lorsque vous créez initialement un nouvel objet, cette date reflète la date à laquelle l'objet a été créé. Si vous remplacez l'objet, la date change en conséquence. Par conséquent, la date de création est synonyme de la date Dernière modification.

Lorsqu'un nombre de jours est spécifié dans les actions `NoncurrentVersionTransition` et `NoncurrentVersionExpiration` dans une configuration du cycle de vie, notez ce qui suit :

- La valeur que vous spécifiez correspond au nombre de jours depuis le moment où l'objet devient non actuel (c'est-à-dire, depuis que l'objet a été remplacé ou supprimé) pendant lesquels Amazon S3 effectuera l'action sur l'objet ou les objets spécifiés.
- Amazon S3 calcule l'heure en ajoutant le nombre de jours spécifié dans la règle à l'heure à laquelle la nouvelle version suivante de l'objet est créée et en arrondissant le temps obtenu au jour suivant à minuit UTC. Par exemple, dans votre compartiment, supposons que vous ayez une version actuelle d'un objet, créée le 01/01/2014 à 10 h 30 UTC. Si la nouvelle version de l'objet qui remplace la version actuelle a été créée le 15/01/2014 à 10 h 30 UTC et que vous spécifiez 3 jours dans une règle de transition, la date de transition de l'objet sera le 19/01/2014 à 00 h 00 UTC.

Règles de cycle de vie : en fonction d'une date spécifique

Lorsqu'une action est spécifiée dans une règle de cycle de vie S3, vous pouvez spécifier la date à laquelle vous souhaitez qu'Amazon S3 exécute l'action. Lorsque la date spécifiée arrive, Amazon S3 applique l'action à tous les objets qualifiés (en fonction des critères de filtre).

Si vous spécifiez une action de cycle de vie S3 avec une date déjà passée, tous les objets qualifiés deviennent immédiatement éligibles pour cette action de cycle de vie.

> **Important**
>
> L'action basée sur la date n'est pas une action unique. Amazon S3 continue à appliquer l'action basée sur la date même après que la date est passée, tant que l'état de la règle est `Enabled`.
>
> Par exemple, supposons que vous spécifiez une action `Expiration` basée sur la date pour supprimer tous les objets (en supposant qu'aucun filtre n'est spécifié dans la règle). À la date spécifiée, Amazon S3 fait expirer tous les objets du compartiment. Amazon S3 continue également à faire expirer tous les nouveaux objets que vous créez dans le compartiment. Pour arrêter cette action de cycle de vie, vous devez supprimer l'action de la configuration du cycle de vie, désactiver la règle ou supprimer la règle de la configuration du cycle de vie.

La valeur de date doit être conforme au format ISO 8601. L'heure indique toujours minuit UTC.

> **Note**
>
> Vous ne pouvez pas créer des règles de cycle de vie basées sur la date en utilisant la console Amazon S3, mais vous pouvez afficher, désactiver ou supprimer ces règles.

Ajout de filtres à des règles de cycle de vie

Les filtres sont un élément facultatif de règle de cycle de vie que vous pouvez utiliser pour spécifier les objets auxquels la règle s'applique.

Les éléments suivants peuvent être utilisés pour filtrer les objets :

Préfixe de clé

Vous pouvez filtrer les objets en fonction d'un préfixe. Si vous souhaitez appliquer une action du cycle de vie à un sous-ensemble d'objets avec des préfixes différents, créez des règles distinctes pour chaque action.

Balises d'objet

Vous pouvez filtrer les objets en fonction d'une ou de plusieurs balises. Chaque balise doit correspondre exactement à la clé et à la valeur et, si vous spécifiez plusieurs balises, chaque clé de balise doit être unique. Un filtre avec plusieurs balises d'objet s'applique à un sous-ensemble d'objets dont toutes les balises sont spécifiées. Si un objet dispose de balises supplémentaires spécifiées, le filtre continue de s'appliquer.

> **Note**
>
> Si vous spécifiez uniquement un élément `Key` et aucun élément `Value`, la règle ne s'applique qu'aux objets correspondant à la clé de balise et pour lesquels aucune valeur n'est spécifiée.

Taille d'objet minimale ou maximale

Vous pouvez filtrer les objets en fonction de leur taille. Vous pouvez spécifier une taille minimale (`ObjectSizeGreaterThan`) ou une taille maximale (`ObjectSizeLessThan`), ou vous pouvez spécifier une plage de tailles d'objet dans le même filtre. Les valeurs de taille d'objet sont exprimées en octets. La taille de filtre maximale est de 5 To. Amazon S3 applique une taille d'objet minimale par défaut à la configuration du cycle de vie. Pour de plus amples informations, veuillez consulter Exemple : permettre la transition d'objets de moins de 128 Ko.

Vous pouvez combiner différents éléments de filtre, auquel cas Amazon S3 utilise un opérateur AND logique.

Exemples de filtre

Les exemples suivants montrent comment vous pouvez utiliser différents éléments de filtre :

- Spécification d'un filtre à l'aide de préfixes de clé : cet exemple montre une règle de cycle de vie S3 qui s'applique à un sous-ensemble d'objets en fonction du préfixe du nom de clé (`logs/`). Par exemple, la règle de cycle de vie s'applique aux objets `logs/mylog.txt`, `logs/temp1.txt` et `logs/test.txt`. La règle ne s'applique pas à l'objet `example.jpg`.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>logs/</Prefix>
```

```
        </Filter>
        transition/expiration actions
         ...
    </Rule>
    ...
</LifecycleConfiguration>
```

> **Note**
>
> Si un ou plusieurs préfixes commencent par les mêmes caractères, vous pouvez inclure tous ces préfixes dans votre règle en spécifiant un préfixe partiel sans barre oblique (/) dans le filtre. Par exemple, supposons que vous avez les préfixes suivants :
>
> ```
> sales1999/
>                sales2000/
>                sales2001/
> ```
>
> Pour inclure ces trois préfixes dans votre règle, spécifiez `sales` comme préfixe dans votre règle de cycle de vie.

Si vous souhaitez appliquer une action de cycle de vie à un sous-ensemble d'objets en fonction de préfixes de noms de clé différents, spécifiez des règles distinctes. Dans chaque règle, spécifiez un filtre basé sur le préfixe. Par exemple, pour décrire une action de cycle de vie pour les objets avec les préfixes de clé `projectA/` et `projectB/`, vous spécifiez deux règles comme suit :

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Prefix>projectA/</Prefix>
        </Filter>
        transition/expiration actions
         ...
    </Rule>

    <Rule>
        <Filter>
           <Prefix>projectB/</Prefix>
        </Filter>
        transition/expiration actions
```

```
        ...
    </Rule>
</LifecycleConfiguration>
```

Pour en savoir plus sur les clés d'objet, consultez Attribution d'un nom aux objets Amazon S3.

- Spécification d'un filtre en fonction de balises d'objet : dans l'exemple suivant, la règle de cycle de vie spécifie un filtre basé sur une balise (*key*) et une valeur (*value*). La règle s'applique ensuite uniquement à un sous-ensemble d'objets avec la balise spécifique.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
           <Tag>
              <Key>key</Key>
              <Value>value</Value>
           </Tag>
        </Filter>
        transition/expiration actions
        ...
    </Rule>
</LifecycleConfiguration>
```

Vous pouvez spécifier un filtre basé sur plusieurs balises. Vous devez encapsuler les balises dans l'élément <And>, comme illustré dans l'exemple suivant. La règle indique à Amazon S3 d'exécuter des actions de cycle de vie sur des objets avec deux balises (avec la clé de balise et la valeur spécifiques).

```
<LifecycleConfiguration>
    <Rule>
      <Filter>
         <And>
            <Tag>
               <Key>key1</Key>
               <Value>value1</Value>
            </Tag>
            <Tag>
               <Key>key2</Key>
               <Value>value2</Value>
            </Tag>
             ...
          </And>
```

```
      </Filter>
      transition/expiration actions
    </Rule>
</Lifecycle>
```

La règle de cycle de vie s'applique aux objets qui ont tous deux des balises spécifiées. Amazon S3 effectue une opération logique AND. Remarques :

- Chaque balise doit correspondre exactement à la fois à la clé et à la valeur. Si vous spécifiez uniquement un élément <Key> et aucun élément <Value>, la règle ne s'applique qu'aux objets correspondant à la clé de balise et pour lesquels aucune valeur n'est spécifiée.
- La règle s'applique à un sous-ensemble d'objets dont toutes les étiquettes sont spécifiées dans la règle. Si un objet dispose d'étiquettes supplémentaires spécifiées, la règle continue à s'appliquer.

> **Note**
>
> Lorsque vous spécifiez plusieurs balises dans un filtre, chaque clé de balise doit être unique.

- Spécification d'un filtre basé à la fois sur le préfixe et sur une ou plusieurs balises : dans une règle de cycle de vie, vous pouvez spécifier un filtre basé à la fois sur le préfixe de clé et sur une ou plusieurs balises. Là encore, vous devez encapsuler tous ces éléments de filtre dans l'élément <And>, comme suit :

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
          <And>
             <Prefix>key-prefix</Prefix>
             <Tag>
                <Key>key1</Key>
                <Value>value1</Value>
             </Tag>
             <Tag>
                <Key>key2</Key>
                <Value>value2</Value>
             </Tag>
              ...
          </And>
        </Filter>
```

```
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Amazon S3 associe ces filtres à l'aide d'un opérateur logique AND. Autrement dit, la règle s'applique au sous-ensemble des objets dotés du préfixe de clé spécifié et des balises spécifiées. Un filtre peut avoir seulement un préfixe et zéro, une ou plusieurs balises.

- Spécification d'un filtre vide : vous pouvez spécifier un filtre vide, auquel cas la règle s'applique à tous les objets dans le compartiment.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

- Spécification d'un filtre de taille d'objet : pour filtrer une règle par taille d'objet, vous pouvez spécifier une taille minimale (`ObjectSizeGreaterThan`) ou une taille maximale (`ObjectSizeLessThan`), ou vous pouvez spécifier une plage de tailles d'objet.

  Les valeurs de taille d'objet sont exprimées en octets. La taille de filtre maximale est de 5 To. Certaines classes de stockage présentent des limites concernant la taille minimale des objets. Pour de plus amples informations, veuillez consulter Comparaison des classes de stockage Amazon S3.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> Les filtres `ObjectSizeGreaterThan` et `ObjectSizeLessThan` excluent les valeurs spécifiées. Par exemple, si vous définissez que les objets d'une taille comprise entre 128 Ko et 1 024 Ko doivent passer de la classe de stockage S3 Standard à la classe de stockage S3 Standard-IA, les objets qui font exactement 1 024 Ko ou 128 Ko ne passeront pas à S3 Standard-IA. À la place, la règle s'appliquera uniquement aux objets de plus de 128 Ko et de moins de 1 024 Ko.

Si vous spécifiez une plage de tailles d'objet, l'entier `ObjectSizeGreaterThan` doit être inférieur à la valeur `ObjectSizeLessThan`. Si vous utilisez plusieurs filtres, vous devez les envelopper dans un élément <And>. L'exemple suivant montre comment spécifier des objets dans une plage comprise entre 500 et 64 000 octets.

```
<LifecycleConfiguration>
    <Rule>
        <Filter>
            <And>
                <Prefix>key-prefix</Prefix>
                <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
                <ObjectSizeLessThan>64000</ObjectSizeLessThan>
            </And>
        </Filter>
        <Status>Enabled</Status>
        transition/expiration actions
    </Rule>
</LifecycleConfiguration>
```

Comment Amazon S3 gère les conflits dans les configurations du cycle de vie

En général, le cycle de vie Amazon S3 optimise les coûts. Par exemple, si deux stratégies d'expiration se chevauchent, la stratégie d'expiration la plus courte est appliquée pour que des données ne soient pas stockées plus longtemps que prévu. De même, si deux stratégies de transition se chevauchent, le cycle de vie S3 effectue la transition de vos objets vers la classe de stockage au coût le plus bas.

Dans les deux cas, le cycle de vie S3 tente de choisir ce qui est le moins cher pour vous. La classe de stockage S3 Intelligent-Tiering (Hiérarchisation intelligente) constitue une exception à cette règle générale. Le cycle de vie S3 privilégie la classe de stockage S3 Intelligent-Tiering (Hiérarchisation intelligente) par rapport à n'importe quelle classe de stockage, à l'exception des classes de stockage S3 Glacier et S3 Glacier Deep Archive.

Si vous avez plusieurs règles dans une configuration du cycle de vie S3, un objet peut devenir éligible pour plusieurs actions du cycle de vie S3 le même jour. Dans de tels cas, Amazon S3 suit les règles générales suivantes :

- La suppression permanente a priorité sur la transition.
- La transition a priorité sur la création de marqueurs de suppression.
- Si un objet est éligible pour les transitions vers S3 Glacier Flexible Retrieval et S3 Standard-IA (ou S3 One Zone-IA), Amazon S3 choisit la transition vers S3 Glacier Flexible Retrieval.

Exemples de chevauchement de filtres et d'actions de cycle de vie contradictoires

Vous pouvez définir une configuration de cycle de vie S3 dans laquelle vous spécifiez des préfixes ou des actions se chevauchant. Les exemples suivants illustrent comment Amazon S3 résout les conflits potentiels.

Example 1 : Chevauchement de préfixes (aucun conflit)

L'exemple de configuration suivant comporte deux règles qui indiquent des préfixes qui se chevauchent comme suit :

- La première règle spécifie un filtre vide, indiquant tous les objets du compartiment.
- La deuxième règle spécifie un préfixe de nom de clé (`logs/`), indiquant uniquement un sous-ensemble d'objets.

La règle 1 demande à Amazon S3 de supprimer tous les objets un an après leur création. La règle 2 demande à Amazon S3 d'effectuer la transition d'un sous-ensemble d'objets vers la classe de stockage S3 standard – Accès peu fréquent 30 jours après la création.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
    <Filter>
```

```
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>30</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

Comme il n'y a pas de conflit dans ce cas, Amazon S3 effectue la transition des objets avec le préfixe `logs/` vers la classe de stockage S3 standard – Accès peu fréquent 30 jours après leur création. Les objets sont ensuite supprimés un an après leur création.

Example 2 : Actions de cycle de vie contradictoires

Dans cet exemple de configuration, il existe deux règles qui indiquent à Amazon S3 d'effectuer en même temps deux actions différentes sur le même ensemble d'objets pendant la durée de vie des objets :

- Les deux règles spécifient le même préfixe de nom de clé et les deux règles s'appliquent par conséquent au même ensemble d'objets.
- Les deux règles spécifient les mêmes 365 jours après la création de l'objet lorsque les règles s'appliquent.
- Une règle indique à Amazon S3 d'effectuer la transition d'objets vers la classe de stockage S3 standard – Accès peu fréquent et une autre règle veut qu'Amazon S3 fasse expirer les objets en même temps.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
```

```
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

Dans ce cas, étant donné que vous voulez que les objets expirent (soient supprimés), il est inutile de modifier la classe de stockage. Par conséquent, Amazon S3 choisit l'action d'expiration sur ces objets.

Example 3 : Chevauchement de préfixes entraînant des actions de cycle de vie contradictoires

Dans cet exemple, la configuration comporte deux règles qui indiquent des préfixes qui se chevauchent comme suit :

- La règle 1 spécifie un préfixe vide (indiquant tous les objets).
- La règle 2 spécifie un préfixe de nom de clé (`logs/`) qui identifie un sous-ensemble de tous les objets.

Pour le sous-ensemble d'objets avec le préfixe de nom de clé `logs/`, les actions de cycle de vie S3 dans les deux règles s'appliquent. Une règle indique à Amazon S3 d'effectuer la transition des objets 10 jours après leur création et une autre règle indique à Amazon S3 d'effectuer la transition des objets 365 jours après leur création.

```
<LifecycleConfiguration>
  <Rule>
```

```
    <ID>Rule 1</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>10</Days>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>STANDARD_IA</StorageClass>
      <Days>365</Days>
    </Transition>
   </Rule>
</LifecycleConfiguration>
```

Dans ce cas, Amazon S3 choisit d'effectuer leur transition 10 jours après leur création.

Example 4 : Filtrage basé sur des balises et actions du cycle de vie contradictoires générées

Supposons que vous avez la configuration de cycle de vie S3 suivante qui a deux règles, chacune spécifiant un filtre de balise :

- La règle 1 spécifie un filtre basé sur une balise (`tag1/value1`). Cette règle indique à Amazon S3 d'effectuer la transition des objets vers la classe de stockage S3 Glacier Flexible Retrieval 365 jours après leur création.
- La règle 2 spécifie un filtre basé sur une balise (`tag2/value2`). Cette règle indique à Amazon S3 de faire expirer les objets 14 jours après leur création.

La configuration de cycle de vie S3 est illustrée dans l'exemple suivant.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule 1</ID>
```

```
    <Filter>
      <Tag>
         <Key>tag1</Key>
         <Value>value1</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <StorageClass>GLACIER</StorageClass>
      <Days>365</Days>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule 2</ID>
    <Filter>
      <Tag>
         <Key>tag2</Key>
         <Value>value2</Value>
      </Tag>
    </Filter>
    <Status>Enabled</Status>
    <Expiration>
      <Days>14</Days>
    </Expiration>
   </Rule>
</LifecycleConfiguration>
```

Si un objet possède les deux balises, Amazon S3 doit décider de la règle à suivre. Dans ce cas, Amazon S3 fait expirer l'objet 14 jours après sa création. L'objet est supprimé et, par conséquent, l'action de transition ne s'applique pas.

Exemples de configurations du cycle de vie S3

Cette section fournit des exemples de configuration de cycle de vie S3. Chaque exemple indique comment vous pouvez spécifier XML dans chaque exemple de scénarios.

Rubriques

- Archivage de tous les objets dans un délai d'un jour après leur création
- Désactivation temporaire des règles du cycle de vie
- Choix d'une classe de stockage inférieure pendant la durée de vie d'un objet

- Spécification de plusieurs règles
- Spécification d'une règle de cycle de vie pour un compartiment avec gestion des versions
- Suppression des marqueurs de suppression des objets expirés dans un compartiment avec gestion des versions
- Configuration du cycle de vie pour annuler les chargements partitionnés
- Expiration d'objets non actuels ne contenant aucune donnée
- Exemple : permettre la transition d'objets de moins de 128 Ko

Archivage de tous les objets dans un délai d'un jour après leur création

Chaque règle de cycle de vie S3 comprend un filtre que vous pouvez utiliser pour identifier un sous-ensemble d'objets dans votre compartiment auquel s'applique la règle de cycle de vie S3. Les configurations S3 de cycle de vie suivantes présentent des exemples de spécification d'un filtre.

- Dans cette règle de configuration de cycle de vie S3, le filtre spécifie un préfixe de clé (`tax/`). Par conséquent, la règle s'applique aux objets avec le préfixe de nom de clé `tax/`, comme `tax/doc1.txt` et `tax/doc2.txt`.

  La règle spécifie deux actions qui demandent à Amazon S3 de procéder comme suit :

  - La transition d'objets vers la classe de stockage S3 Glacier Flexible Retrieval 365 jours (un an) après leur création.
  - La suppression d'objets (l'action `Expiration`) 3 650 jours (10 ans) après leur création.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition and Expiration Rule</ID>
    <Filter>
       <Prefix>tax/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
    <Expiration>
      <Days>3650</Days>
    </Expiration>
  </Rule>
```

```
</LifecycleConfiguration>
```

Au lieu de spécifier l'âge de l'objet en termes de jours après sa création, vous pouvez spécifier une date pour chaque action. Cependant, vous ne pouvez pas utiliser à la fois `Date` et `Days` dans la même règle.

- Si vous souhaitez que la règle de cycle de vie S3 s'applique à tous les objets dans le compartiment, spécifiez un préfixe vide. Dans la configuration suivante, la règle spécifie une action `Transition` qui indique à Amazon S3 d'effectuer la transition des objets vers la classe de stockage S3 Glacier Flexible Retrieval 0 jour après leur création. Cette règle signifie que les objets sont éligibles pour l'archivage dans S3 Glacier Flexible Retrieval à minuit UTC après leur création. Pour d'informations sur les contraintes de cycle de vie, consultez Contraintes et considérations pour les transitions.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Archive all object same-day upon creation</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

- Vous pouvez spécifier un préfixe de nom de clé, ou aucun, et plusieurs balises d'objets dans un filtre, ou aucune. L'exemple de code suivant applique la règle de cycle de vie S3 à un sous-ensemble d'objets avec le préfixe de clé `tax/` et aux objets ayant deux balises avec une clé et une valeur spécifiques. Si vous spécifiez plusieurs filtres, vous devez inclure l'élément <And> comme illustré (Amazon S3 applique un opérateur logique AND pour combiner les conditions de filtre spécifiées).

```
...
<Filter>
   <And>
      <Prefix>tax/</Prefix>
      <Tag>
         <Key>key1</Key>
```

```
         <Value>value1</Value>
      </Tag>
      <Tag>
         <Key>key2</Key>
         <Value>value2</Value>
      </Tag>
    </And>
</Filter>
...
```

- Vous pouvez filtrer des objets en fonction uniquement des balises. Par exemple, la règle de cycle de vie S3 suivante s'applique aux objets ayant les deux balises spécifiées (elle ne spécifie pas de préfixe).

```
...
<Filter>
   <And>
      <Tag>
         <Key>key1</Key>
         <Value>value1</Value>
      </Tag>
      <Tag>
         <Key>key2</Key>
         <Value>value2</Value>
      </Tag>
    </And>
</Filter>
...
```

Important

Si vous avez plusieurs règles dans une configuration du cycle de vie S3, un objet peut devenir éligible pour plusieurs actions du cycle de vie S3 le même jour. Dans de tels cas, Amazon S3 suit les règles générales suivantes :

- La suppression permanente a priorité sur la transition.
- La transition a priorité sur la création de marqueurs de suppression.

- Si un objet est éligible pour les transitions vers S3 Glacier Flexible Retrieval et S3 Standard-IA (ou S3 One Zone-IA), Amazon S3 choisit la transition vers S3 Glacier Flexible Retrieval.

Pour obtenir des exemples, consultez Exemples de chevauchement de filtres et d'actions de cycle de vie contradictoires.

Désactivation temporaire des règles du cycle de vie

Vous pouvez désactiver temporairement une règle du cycle de vie S3 à l'aide de l'élément `status`. Cela peut être utile si vous souhaitez tester de nouvelles règles ou résoudre des problèmes liés à votre configuration, sans remplacer vos règles existantes. La configuration de cycle de vie S3 suivante spécifie deux règles :

- La règle 1 indique à Amazon S3 d'effectuer la transition des objets avec le préfixe `logs/` vers la classe de stockage S3 Glacier Flexible Retrieval peu de temps après leur création.
- La règle 2 indique à Amazon S3 d'effectuer la transition des objets avec le préfixe `documents/` vers la classe de stockage S3 Glacier Flexible Retrieval peu de temps après leur création.

Dans la configuration, la règle 1 est activée et la règle 2 est désactivée. Amazon S3 ignore la règle désactivée.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Rule1</ID>
    <Filter>
      <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
  <Rule>
    <ID>Rule2</ID>
    <Filter>
```

```
      <Prefix>documents/</Prefix>
    </Filter>
    <Status>Disabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Choix d'une classe de stockage inférieure pendant la durée de vie d'un objet

Dans cet exemple, vous utilisez une configuration de cycle de vie S3 pour faire passer des objets à la classe de stockage inférieure pendant leur cycle de vie. Ce choix peut permettre de réduire les coûts de stockage. Pour plus d'informations sur la tarification, consultez Tarification Amazon S3.

L'exemple suivant de configuration de cycle de vie S3 spécifie une règle qui s'applique aux objets avec le préfixe de nom de clé `logs/`. La règle spécifie les deux actions suivantes :

- Deux actions de transition :
  - La transition d'objets vers la classe de stockage S3 standard – Accès peu fréquent 30 jours après leur création.
  - La transition d'objets vers la classe de stockage S3 Glacier Flexible Retrieval 90 jours après leur création.
- Une action d'expiration qui indique à Amazon S3 de supprimer les objets un an après leur création.

```
<LifecycleConfiguration>
  <Rule>
    <ID>example-id</ID>
    <Filter>
       <Prefix>logs/</Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>30</Days>
      <StorageClass>STANDARD_IA</StorageClass>
    </Transition>
    <Transition>
      <Days>90</Days>
      <StorageClass>GLACIER</StorageClass>
```

```
    </Transition>
    <Expiration>
      <Days>365</Days>
    </Expiration>
  </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> Vous pouvez utiliser une règle pour décrire toutes les actions de cycle de vie S3 si toutes les actions s'appliquent au même ensemble d'objets (identifié par le filtre). Sinon, vous pouvez ajouter plusieurs règles, chacune spécifiant un filtre différent.

> **Important**
>
> Si vous avez plusieurs règles dans une configuration du cycle de vie S3, un objet peut devenir éligible pour plusieurs actions du cycle de vie S3 le même jour. Dans de tels cas, Amazon S3 suit les règles générales suivantes :
>
> - La suppression permanente a priorité sur la transition.
> - La transition a priorité sur la création de marqueurs de suppression.
> - Si un objet est éligible pour les transitions vers S3 Glacier Flexible Retrieval et S3 Standard-IA (ou S3 One Zone-IA), Amazon S3 choisit la transition vers S3 Glacier Flexible Retrieval.
>
> Pour obtenir des exemples, consultez Exemples de chevauchement de filtres et d'actions de cycle de vie contradictoires.

Spécification de plusieurs règles

Vous pouvez spécifier plusieurs règles si vous souhaitez effectuer différentes actions de cycle de vie S3 pour différents d'objets. La configuration de cycle de vie S3 suivante a deux règles :

- La règle 1 s'applique aux objets ayant le préfixe de nom de clé `classA/`. Elle indique à Amazon S3 d'effectuer la transition d'objets vers la classe de stockage S3 Glacier Flexible Retrieval un an après leur création et de faire expirer ces objets 10 ans après leur création.
- La règle 2 s'applique aux objets ayant le préfixe de nom de clé `classB/`. Elle indique à Amazon S3 d'effectuer la transition d'objets vers la classe de stockage S3 standard – Accès peu fréquent 90 jours après leur création et de les supprimer un an après leur création.

```
<LifecycleConfiguration>
    <Rule>
        <ID>ClassADocRule</ID>
        <Filter>
           <Prefix>classA/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>365</Days>
           <StorageClass>GLACIER</StorageClass>
        </Transition>
        <Expiration>
             <Days>3650</Days>
        </Expiration>
    </Rule>
    <Rule>
        <ID>ClassBDocRule</ID>
        <Filter>
            <Prefix>classB/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <Expiration>
             <Days>365</Days>
        </Expiration>
    </Rule>
</LifecycleConfiguration>
```

Important

Si vous avez plusieurs règles dans une configuration du cycle de vie S3, un objet peut devenir éligible pour plusieurs actions du cycle de vie S3 le même jour. Dans de tels cas, Amazon S3 suit les règles générales suivantes :

- La suppression permanente a priorité sur la transition.
- La transition a priorité sur la création de marqueurs de suppression.
- Si un objet est éligible pour les transitions vers S3 Glacier Flexible Retrieval et S3 Standard-IA (ou S3 One Zone-IA), Amazon S3 choisit la transition vers S3 Glacier Flexible Retrieval.

Pour obtenir des exemples, consultez Exemples de chevauchement de filtres et d'actions de cycle de vie contradictoires.

Spécification d'une règle de cycle de vie pour un compartiment avec gestion des versions

Imaginez que vous avez un compartiment sur lequel la gestion des versions est activée. Dans ce cas, vous avez pour chaque objet une version actuelle et éventuellement une ou plusieurs versions anciennes. (Pour plus d'informations sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.)

Dans l'exemple suivant, vous souhaitez conserver un historique d'un an et conserver 5 versions non actuelles. Les configurations du cycle de vie S3 prennent en charge la conservation de 1 à 100 versions de n'importe quel objet. Sachez que plus de 5 nouvelles versions non actuelles doivent exister avant qu'Amazon S3 puisse expirer une version donnée. Amazon S3 supprime définitivement toutes les versions non actuelles supplémentaires au-delà du nombre spécifié à conserver. Pour que la suppression ait lieu, les valeurs `NoncurrentDays` et les `NewerNoncurrentVersions` valeurs doivent être dépassées.

Afin de réaliser des économiser sur les coûts de stockage, vous souhaitez déplacer les versions anciennes vers S3 Glacier Flexible Retrieval 30 jours après qu'elles sont devenues anciennes (en supposant que ces objets anciens sont des données froides auxquelles vous n'avez pas besoin d'accéder en temps réel). En outre, vous vous attendez à ce que la fréquence d'accès des versions

actuelles diminue 90 jours après leur création. Vous pouvez dès lors décider de déplacer ces objets vers la classe de stockage S3 Standard-IA.

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix></Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Transition>
           <Days>90</Days>
           <StorageClass>STANDARD_IA</StorageClass>
        </Transition>
        <NoncurrentVersionTransition>
            <NoncurrentDays>30</NoncurrentDays>
            <StorageClass>GLACIER</StorageClass>
        </NoncurrentVersionTransition>
       <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>5</NewerNoncurrentVersions>
            <NoncurrentDays>365</NoncurrentDays>
       </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

Suppression des marqueurs de suppression des objets expirés dans un compartiment avec gestion des versions

Un compartiment activé pour la gestion des versions a une version d'objet actuelle et une ou plusieurs versions anciennes pour chaque objet. Lorsque vous supprimez un objet, notez ce qui suit :

- Si vous ne spécifiez pas un ID de version dans votre demande de suppression, Amazon S3 ajoute un marqueur de suppression au lieu de supprimer l'objet. La version actuelle de l'objet devient ancienne et le marqueur de suppression devient la version actuelle.
- Si vous spécifiez un ID de version dans votre demande de suppression, Amazon S3 supprime définitivement la version de l'objet (aucun marqueur de suppression n'est créé).
- Un marqueur de suppression avec aucune version ancienne est appelé marqueur de suppression d'objet expiré.

Cet exemple illustre un scénario qui peut créer des marqueurs de suppression d'objet expiré dans votre compartiment et la façon dont vous pouvez utiliser une configuration de cycle de vie S3 pour indiquer à Amazon S3 de supprimer les marqueurs de suppression d'objet expiré.

Supposons que vous écriviez une configuration S3 Lifecycle qui utilise l'`NoncurrentVersionExpiration`action pour supprimer les versions non actuelles 30 jours après leur disparition et pour conserver 10 versions non actuelles, comme indiqué dans l'exemple suivant. Sachez que plus de 10 nouvelles versions non actuelles doivent exister avant qu'Amazon S3 puisse expirer une version donnée. Amazon S3 supprime définitivement toutes les versions non actuelles supplémentaires au-delà du nombre spécifié à conserver. Pour que la suppression ait lieu, les valeurs `NoncurrentDays` et les `NewerNoncurrentVersions` valeurs doivent être dépassées.

```
<LifecycleConfiguration>
    <Rule>
        ...
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

L'`NoncurrentVersionExpiration`action ne s'applique pas aux versions actuelles de l'objet. Elle supprime uniquement les versions anciennes.

Pour les versions d'objet actuelles, les options suivantes vous permettent de gérer leur cycle de vie selon que les versions d'objet actuelles suivent un cycle de vie bien défini :

- Les versions d'objet actuelles suivent un cycle de vie bien défini.

  Dans ce cas, vous pouvez utiliser une configuration de cycle de vie S3 avec l'action `Expiration` pour indiquer à Amazon S3 de supprimer les versions actuelles, comme illustré dans l'exemple suivant.

  ```
  <LifecycleConfiguration>
      <Rule>
          ...
          <Expiration>
             <Days>60</Days>
          </Expiration>
          <NoncurrentVersionExpiration>
  ```

```
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

Dans cet exemple, Amazon S3 supprime les versions actuelles 60 jours après leur création en ajoutant un marqueur de suppression pour chacune des versions d'objet actuelles. Ainsi, la version actuelle devient ancienne et le marqueur de suppression devient la version actuelle. Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

> **Note**
>
> Vous ne pouvez pas spécifier à la fois un `Days` et un `ExpiredObjectDeleteMarker` tag sur la même règle. Si vous spécifiez la balise `Days`, Amazon S3 effectue automatiquement le nettoyage `ExpiredObjectDeleteMarker` une fois que les marqueurs de suppression sont suffisamment anciens pour satisfaire aux critères d'âge. Pour nettoyer les marqueurs de suppression dès qu'ils deviennent la seule version, créez une règle distincte avec uniquement la balise `ExpiredObjectDeleteMarker`.

L'action `NoncurrentVersionExpiration` dans la même configuration de cycle de vie S3 supprime les objets anciens 30 jours après qu'ils sont devenus anciens. Ainsi, dans cet exemple, toutes les versions d'objet sont définitivement supprimées 90 jours après la création de l'objet. Sachez que dans cet exemple, plus de 10 nouvelles versions non actuelles doivent exister avant qu'Amazon S3 puisse expirer une version donnée. Amazon S3 supprime définitivement toutes les versions non actuelles supplémentaires au-delà du nombre spécifié à conserver. Pour que la suppression ait lieu, les valeurs `NoncurrentDays` et les `NewerNoncurrentVersions` valeurs doivent être dépassées.

Bien que des marqueurs de suppression d'objet expiré soient créés au cours de ce processus, Amazon S3 détecte et supprime les marqueurs de suppression d'objet expiré à votre place.

- Les versions d'objet actuelles n'ont pas de cycle de vie bien défini.

  Dans ce cas, vous pouvez supprimer les objets manuellement si vous n'en avez pas besoin, ce qui créera un marqueur de suppression avec une ou plusieurs versions anciennes. Si la configuration

de cycle de vie S3 avec l'action `NoncurrentVersionExpiration` supprime toutes les versions anciennes, vous avez à présent des marqueurs de suppression d'objet expiré.

Plus précisément pour ce scénario, la configuration de cycle de vie S3 fournit une action `Expiration` que vous pouvez utiliser pour supprimer les marqueurs de suppression d'objet expiré.

```
<LifecycleConfiguration>
    <Rule>
       <ID>Rule 1</ID>
        <Filter>
          <Prefix>logs/</Prefix>
        </Filter>
        <Status>Enabled</Status>
        <Expiration>
           <ExpiredObjectDeleteMarker>true</ExpiredObjectDeleteMarker>
        </Expiration>
        <NoncurrentVersionExpiration>
            <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
            <NoncurrentDays>30</NoncurrentDays>
        </NoncurrentVersionExpiration>
    </Rule>
</LifecycleConfiguration>
```

En définissant l'élément `ExpiredObjectDeleteMarker` sur `true` dans l'action `Expiration`, vous indiquez à Amazon S3 de supprimer les marqueurs de suppression d'objet expiré.

> **Note**
>
> Si vous spécifiez l'action de cycle de vie S3 `ExpiredObjectDeleteMarker`, la règle ne peut pas spécifier un filtre basé sur une balise.

Configuration du cycle de vie pour annuler les chargements partitionnés

Vous pouvez utiliser les opérations d'API REST de chargement partitionné Amazon S3 pour charger des objets volumineux en plusieurs parties. Pour en savoir plus sur les chargements partitionnés, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Avec une configuration du cycle de vie S3, vous pouvez indiquer à Amazon S3 d'arrêter les chargements partitionnés incomplets (identifiés par le préfixe de nom de clé spécifié dans la règle) s'ils ne se terminent pas avant un certain nombre de jours suivant leur lancement. Lorsque Amazon S3 interrompt un chargement partitionné, toutes les parties associées au chargement partitionné sont supprimées. Ce processus vous aide à contrôler vos coûts de stockage en garantissant que vous n'avez pas de chargements partitionnés incomplets avec des parties stockées dans Amazon S3.

> **Note**
>
> Si vous spécifiez l'action de cycle de vie S3 `AbortIncompleteMultipartUpload`, la règle ne peut pas spécifier un filtre basé sur une balise.

Voici un exemple de configuration de cycle de vie S3 qui spécifie une règle avec l'action `AbortIncompleteMultipartUpload`. Cette action indique à Amazon S3 d'arrêter les chargements partitionnés incomplets sept jours après leur lancement.

```
<LifecycleConfiguration>
    <Rule>
        <ID>sample-rule</ID>
        <Filter>
           <Prefix>SomeKeyPrefix/</Prefix>
        </Filter>
        <Status>rule-status</Status>
        <AbortIncompleteMultipartUpload>
          <DaysAfterInitiation>7</DaysAfterInitiation>
        </AbortIncompleteMultipartUpload>
    </Rule>
</LifecycleConfiguration>
```

Expiration d'objets non actuels ne contenant aucune donnée

Vous pouvez créer des règles qui transfèrent des objets uniquement en fonction de leur taille. Vous pouvez spécifier une taille minimale (`ObjectSizeGreaterThan`) ou une taille maximale (`ObjectSizeLessThan`), ou vous pouvez spécifier une plage de tailles d'objet en octets. Si vous utilisez plusieurs filtres, comme une règle de préfixe et de taille, vous devez les envelopper dans un élément <And>.

```
<LifecycleConfiguration>
```

```
  <Rule>
    <ID>Transition with a prefix and based on size</ID>
    <Filter>
       <And>
          <Prefix>tax/</Prefix>
          <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
       </And>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Si vous spécifiez une plage en utilisant à la fois les éléments `ObjectSizeGreaterThan` et `ObjectSizeLessThan`, la taille maximale des objets doit être supérieure à la taille minimale des objets. Si vous utilisez plusieurs filtres, vous devez les envelopper dans un élément <And>. L'exemple suivant montre comment spécifier des objets dans une plage comprise entre 500 et 64 000 octets. Lorsque vous spécifiez une plage, les filtres `ObjectSizeGreaterThan` et `ObjectSizeLessThan` excluent les valeurs spécifiées. Pour de plus amples informations, veuillez consulter the section called "Élément de filtre".

```
<LifecycleConfiguration>
    <Rule>
        ...
          <And>
             <ObjectSizeGreaterThan>500</ObjectSizeGreaterThan>
             <ObjectSizeLessThan>64000</ObjectSizeLessThan>
          </And>
    </Rule>
</LifecycleConfiguration>
```

Vous pouvez également créer des règles pour faire expirer spécifiquement les anciens objets qui ne contiennent aucune donnée, y compris les anciens objets marqueurs de suppression, créés dans un compartiment doté de la gestion des versions. L'exemple suivant utilise l'`NoncurrentVersionExpiration`action pour supprimer les versions non actuelles 30 jours après leur disparition et pour conserver 10 versions non actuelles. Cet exemple utilise également l'`ObjectSizeLessThan`élément pour filtrer uniquement les objets dépourvus de données.

Sachez que plus de 10 nouvelles versions non actuelles doivent exister avant qu'Amazon S3 puisse expirer une version donnée. Amazon S3 supprime définitivement toutes les versions non actuelles supplémentaires au-delà du nombre spécifié à conserver. Pour que la suppression ait lieu, les valeurs `NoncurrentDays` et les `NewerNoncurrentVersions` valeurs doivent être dépassées.

```
<LifecycleConfiguration>
  <Rule>
    <ID>Expire noncurrent with size less than 1 byte</ID>
    <Filter>
       <ObjectSizeLessThan>1</ObjectSizeLessThan>
    </Filter>
    <Status>Enabled</Status>
    <NoncurrentVersionExpiration>
       <NewerNoncurrentVersions>10</NewerNoncurrentVersions>
       <NoncurrentDays>30</NoncurrentDays>
    </NoncurrentVersionExpiration>
  </Rule>
</LifecycleConfiguration>
```

Exemple : permettre la transition d'objets de moins de 128 Ko

Amazon S3 applique un comportement par défaut à votre configuration du cycle de vie qui empêche la transition des objets de moins de 128 Ko vers toute classe de stockage. Vous pouvez autoriser la transition des objets plus petits en ajoutant un filtre de taille minimale (`ObjectSizeGreaterThan`) ou de taille maximale (`ObjectSizeLessThan`) qui spécifie une taille inférieure pour la configuration. L'exemple suivant permet la transition de tout objet de moins de 128 Ko vers la classe de stockage S3 Glacier Instant Retrieval :

```
<LifecycleConfiguration>
  <Rule>
    <ID>Allow small object transitions</ID>
    <Filter>
          <ObjectSizeGreaterThan>1</ObjectSizeGreaterThan>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>365</Days>
      <StorageClass>GLACIER_IR</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

> **Note**
>
> En septembre 2024, Amazon S3 a mis à jour le comportement de transition par défaut pour les petits objets, comme suit :
>
> - Comportement de transition par défaut mis à jour : à compter du mois de septembre 2024, le comportement par défaut empêche les objets de moins de 128 Ko d'être transférés vers toute classe de stockage.
> - Comportement de transition par défaut précédent : avant le mois de septembre 2024, le comportement par défaut autorisait les objets de moins de 128 Ko à être transférés uniquement vers les classes de stockage S3 Glacier et S3 Glacier Deep Archive.
>
> Les configurations créées avant le mois de septembre 2024 conservent le comportement de transition précédent, sauf si vous les modifiez. En d'autres termes, si vous créez, modifiez ou supprimez des règles, le comportement de transition par défaut de votre configuration est remplacé par le comportement mis à jour. Si votre cas d'utilisation l'exige, vous pouvez modifier le comportement de transition par défaut afin que les objets de moins de 128 Ko soient transférés vers S3 Glacier et S3 Glacier Deep Archive. Pour ce faire, utilisez l'`x-amz-transition-object-size-minimum-default`en-tête facultatif dans un PutBucketLifecycleConfiguration de la demande.

L'exemple suivant montre comment utiliser l'`x-amz-transition-object-size-minimum-default`en-tête dans un PutBucketLifecycleConfigurationdemande d'application du comportement de transition `varies_by_storage_class` par défaut à une configuration S3 Lifecycle. Ce comportement permet aux objets de moins de 128 Ko de passer aux classes de stockage S3 Glacier ou S3 Glacier Deep Archive. Par défaut, toutes les autres classes de stockage empêcheront les transitions inférieures à 128 Ko. Vous pouvez toujours utiliser des filtres personnalisés pour modifier la taille de transition minimale pour une classe de stockage quelconque. Les filtres personnalisés ont toujours priorité sur le comportement de transition par défaut :

```
HTTP/1.1 200
x-amz-transition-object-size-minimum-default: varies_by_storage_class
<?xml version="1.0" encoding="UTF-8"?>
...
```

Résolution des problèmes du cycle de vie Amazon S3

Les informations suivantes peuvent vous aider à résoudre les problèmes courants liés aux règles de cycle de vie Amazon S3.

Rubriques

- J'ai exécuté une opération de liste sur mon compartiment et j'ai vu des objets qui, selon moi, avaient expiré ou avaient été transférés par une règle de cycle de vie.
- Comment puis-je surveiller les actions prises conformément à mes règles de cycle de vie ?
- Le nombre de mes objets S3 continue d'augmenter, même après avoir défini des règles de cycle de vie sur un compartiment avec gestion des versions.
- Comment vider mon compartiment S3 en utilisant des règles de cycle de vie ?
- Ma facture Amazon S3 a augmenté après la transition d'objets vers une classe de stockage moins coûteuse.
- J'ai mis à jour ma politique de compartiment, mais mes objets S3 sont toujours supprimés en raison de règles de cycle de vie expirées.
- Puis-je récupérer des objets S3 expirés conformément aux règles du cycle de vie S3 ?
- Pourquoi les actions relatives à mon cycle de vie d'expiration et de transition ne se produisent-elles pas ?
- Comment puis-je exclure un préfixe de ma règle de cycle de vie ?
- Comment puis-je inclure plusieurs préfixes dans ma règle de cycle de vie ?

J'ai exécuté une opération de liste sur mon compartiment et j'ai vu des objets qui, selon moi, avaient expiré ou avaient été transférés par une règle de cycle de vie.

Les transitions et les expirations d'objets du cycle de vie S3 sont des opérations asynchrones. Par conséquent, il peut y avoir un délai entre le moment où les objets sont éligibles à l'expiration ou à la transition et le moment où ils sont réellement transférés ou ils expirent. Les changements de tarification sont appliqués dès que la règle du cycle de vie est satisfaite, même si l'action n'est pas terminée. Il existe toutefois une exception à ce comportement si vous disposez d'une règle de cycle de vie configurée pour transférer l'objet vers la classe de stockage S3 Intelligent-Tiering. Dans ce cas, les changements de facturation ne se produisent pas tant que l'objet n'est pas passé à la classe de stockage S3 Intelligent-Tiering. Pour plus d'informations sur les changements de facturation, consultez Définition d'une configuration de cycle de vie sur un compartiment.

> **Note**
>
> Amazon S3 ne effectue pas la transition d'objets de moins de 128 Ko vers les classes de stockage S3 Standard ou S3 Standard-IA vers les classes de stockage S3 Intelligent-Tiering, S3 Standard-IA ou S3 One Zone-IA.

Comment puis-je surveiller les actions prises conformément à mes règles de cycle de vie ?

Pour surveiller les actions prises conformément aux règles de cycle de vie, vous pouvez utiliser les fonctionnalités suivantes :

- Notifications d'événements S3 : vous pouvez configurer des notifications d'événements S3 afin d'être informé de tout événement d'expiration ou de transition du cycle de vie S3.
- Journaux d'accès au serveur S3 : vous pouvez activer les journaux d'accès au serveur pour vos compartiments S3 afin de capturer les actions liées au cycle de vie, comme les transitions d'objets vers une autre classe de stockage ou les expirations d'objets. Pour plus d'informations, consultez Cycle de vie et journalisation.

Pour visualiser au quotidien les modifications de votre stockage causées par les actions du cycle de vie, nous vous recommandons d'utiliser les tableaux de bord S3 Storage Lens plutôt que d'utiliser CloudWatch les métriques Amazon. Le tableau de bord Storage Lens vous permet de visualiser les métriques suivantes, qui permettent de surveiller le nombre d'objets ou leur taille :

- Octets de version actuelle
- Nombre d'objets de version actuelle
- Octets de version ancienne
- Nombre d'objets de version ancienne
- Nombre d'objets marqueur de suppression
- Supprimer les octets de stockage des marqueurs
- Octets de chargement partitionné non terminés
- Nombre d'objets de chargement partitionné non terminés

Le nombre de mes objets S3 continue d'augmenter, même après avoir défini des règles de cycle de vie sur un compartiment avec gestion des versions.

Dans un compartiment avec gestion des versions, quand un objet expire, il n'est pas complètement supprimé du compartiment. Au lieu de cela, un marqueur de suppression est créé en tant que version la plus récente de l'objet. Les marqueurs de suppression sont toujours comptés comme des objets. Par conséquent, si une règle de cycle de vie est créée pour faire expirer uniquement les versions actuelles, alors le nombre d'objets dans le compartiment S3 augmente au lieu de diminuer.

Par exemple, supposons qu'un compartiment S3 ait la gestion des versions activée avec 100 objets et qu'une règle de cycle de vie soit définie pour faire expirer les versions actuelles de l'objet au bout de 7 jours. Après le septième jour, le nombre d'objets passe à 200 car 100 marqueurs de suppression sont créés en plus des 100 objets d'origine, qui sont désormais des versions anciennes. Pour plus d'informations sur les actions des règles de configuration du cycle de vie S3 pour les compartiments avec la gestion des versions activée, consultez Définition d'une configuration de cycle de vie sur un compartiment.

Pour supprimer définitivement des objets, ajoutez une configuration de cycle de vie supplémentaire afin de supprimer les versions précédentes des objets, les marqueurs de suppression expirés et les chargements partitionnés incomplets. Pour obtenir des instructions sur la création de nouvelles règles de cycle de vie, consultez Définition d'une configuration de cycle de vie sur un compartiment.

> **Note**
>
> - Amazon S3 arrondit la date de transition ou d'expiration d'un objet à minuit UTC le jour suivant.
>
> Lors de l'évaluation des objets pour les actions de cycle de vie, Amazon S3 utilise l'heure UTC de création des objets. Prenons l'exemple d'un compartiment non versionné doté d'une règle de cycle de vie configurée pour faire expirer les objets au bout d'un jour. Supposons qu'un objet a été créé le 1er janvier à 17 h 05, heure avancée du Pacifique (PDT), ce qui correspond au 2 janvier à 00 h 05 UTC. L'objet est âgé d'un jour à 00 h 05 UTC le 3 janvier, ce qui le rend éligible à l'expiration lorsque S3 Lifecycle évalue les objets à 00 h 00 UTC le 4 janvier.
>
> Comme les actions de cycle de vie Amazon S3 se produisent de manière asynchrone, il peut y avoir un certain retard entre la date spécifiée dans la règle de cycle de vie et la

transition physique réelle de l'objet. Pour plus d'informations, consultez Délai de transition ou d'expiration.

Pour plus d'informations, consultez Règles de cycle de vie : en fonction de l'âge de l'objet.

- Pour les objets S3 protégés par le verrouillage d'objet, les versions actuelles ne sont pas supprimées définitivement. Au lieu de cela, un marqueur de suppression est ajouté aux objets, les rendant anciens. Les versions anciennes sont ensuite conservées et ne sont pas définitivement expirées.

Comment vider mon compartiment S3 en utilisant des règles de cycle de vie ?

Les règles de cycle de vie S3 constituent un outil efficace pour vider un compartiment S3 contenant des millions d'objets. Pour supprimer un nombre important d'objets de votre compartiment S3, veillez à utiliser ces deux paires de règles de cycle de vie :

- Expirer les versions actuelles d'objets et Supprimer définitivement les versions précédentes des objets
- Supprimer les marqueurs de suppression expirés et Supprimer les téléchargements partitionnés non terminés

Pour savoir comment créer une nouvelle règle de configuration du cycle de vie, consultez Définition d'une configuration de cycle de vie sur un compartiment.

> **Note**
>
> Pour les objets S3 protégés par le verrouillage d'objet, les versions actuelles ne sont pas supprimées définitivement. Au lieu de cela, un marqueur de suppression est ajouté aux objets, les rendant anciens. Les versions anciennes sont ensuite conservées et ne sont pas définitivement expirées.

Ma facture Amazon S3 a augmenté après la transition d'objets vers une classe de stockage moins coûteuse.

Votre facture peut augmenter après le transfert d'objets vers une classe de stockage moins coûteuse pour plusieurs raisons :

- Frais généraux de S3 Glacier pour les petits objets

  Pour chaque objet vers les classes de stockage S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive Retrieval, une surcharge totale de 40 Ko est associée à cette mise à jour. Dans le cadre de la surcharge de 40 Ko, 8 Ko sont utilisés pour stocker les métadonnées et le nom de l'objet. Ces 8 Ko sont facturés selon les tarifs S3 Standard. Les 32 Ko restants sont utilisés pour l'indexation et les métadonnées associées. Ces 32 Ko sont facturés selon les tarifs S3 Glacier Flexible Retrieval ou S3 Glacier Deep Archive Retrieval.

  Par conséquent, si vous stockez de nombreux objets de petite taille, nous vous déconseillons d'utiliser des transitions de cycle de vie. Pour réduire les frais de surcharge, envisagez de regrouper de nombreux petits objets en un plus petit nombre de gros objets avant de les stocker dans Amazon S3. Pour plus d'informations sur les considérations de coûts, consultez Transition vers les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive (archivage d'objets).

- Frais de stockage minimaux

  Certaines classes de stockage S3 ont des exigences en matière de durée de stockage minimale. Les objets supprimés, remplacés ou transférés de ces classes avant que la durée minimale ne soit atteinte sont soumis à des frais de transition ou de suppression anticipés au prorata. Ces exigences en matière de durée de stockage minimale sont les suivantes :

  - S3 Standard-IA et S3 One Zone-IA : 30 jours
  - S3 Glacier Flexible Retrieval et S3 Glacier Instant Retrieval – 90 jours
  - S3 Glacier Deep Archive – 180 jours

  Pour plus d'informations sur ces exigences, consultez la section Contraintes de la Transition des objets à l'aide du cycle de vie Amazon S3. Pour plus d'informations générales sur la tarification de S3, consultez Tarification Amazon S3 et Calculateur de tarification AWS.

- Règles de transition du cycle de vie

  Chaque fois qu'un objet est transféré vers une classe de stockage différente selon une règle de cycle de vie, Amazon S3 considère cette transition comme une demande de transition. Les coûts de ces demandes de transition s'ajoutent aux coûts de ces classes de stockage. Si vous envisagez de procéder à la transition d'un grand nombre d'objets, tenez compte des coûts de demande pour une transition vers un niveau inférieur. Pour plus d'informations, consultez Tarification Amazon S3.

J'ai mis à jour ma politique de compartiment, mais mes objets S3 sont toujours supprimés en raison de règles de cycle de vie expirées.

Les déclarations `Deny` figurant dans une politique de compartiment n'empêchent pas l'expiration des objets définis dans une règle de cycle de vie. Les actions du cycle de vie (telles que les transitions ou les expirations) n'utilisent pas l'opération `DeleteObject` S3. Au lieu de cela, les actions du cycle de vie S3 sont effectuées à l'aide de points de terminaison S3 internes. (Pour plus d'informations, consultez Cycle de vie et journalisation.)

Pour empêcher toute action de votre règle de cycle de vie, vous devez la modifier, la supprimer ou la désactiver.

Puis-je récupérer des objets S3 expirés conformément aux règles du cycle de vie S3 ?

Le seul moyen de récupérer des objets expirés conformément au cycle de vie S3 est de procéder à la gestion des versions, qui doit être en place avant que les objets ne puissent être éligibles à l'expiration. Vous ne pouvez pas annuler les opérations d'expiration effectuées par des règles du cycle de vie. Si des objets sont définitivement supprimés conformément aux règles du cycle de vie S3 en vigueur, vous ne pouvez pas récupérer ces objets. Pour activer la gestion des versions sur un compartiment, consultez the section called "Conservation de plusieurs versions d'objets".

Si vous avez appliqué la gestion des versions au compartiment et que les versions anciennes des objets sont toujours intactes, vous pouvez restaurer les versions précédentes des objets expirés. Pour plus d'informations sur le comportement des actions des règles de cycle de vie S3 et les états de gestion des versions, consultez le tableau Actions du cycle de vie et état de la gestion des versions du compartiment dans Éléments pour décrire les actions du cycle de vie.

> **Note**
>
> Si le compartiment S3 est protégé par AWS Backup ou la réplication S3, vous pouvez également utiliser ces fonctionnalités pour récupérer vos objets expirés.

Pourquoi les actions relatives à mon cycle de vie d'expiration et de transition ne se produisent-elles pas ?

Pour un compartiment activé ou suspendu pour les versions, les considérations suivantes indiquent comment Amazon S3 gère l'action d'expiration :

- L'expiration d'objet s'applique uniquement à la version actuelle de l'objet (elle n'a aucun impact sur les versions d'objet non actuelles).
- Amazon S3 n'effectue aucune action en présence d'une ou de plusieurs versions d'objet et si le marqueur de suppression est la version actuelle.
- Amazon S3 n'effectue aucune action sur les versions non actuelles des objets auxquels S3 Object Lock est appliqué.
- Pour les objets dotés d'un statut de `PENDING` réplication, Amazon S3 n'entreprend aucune action sur les versions actuelles ou non actuelles des objets.

Les transitions des classes de stockage de cycle de vie obéissent aux contraintes suivantes :

- Par défaut, les objets d'une taille inférieure à 128 Ko ne seront transférés vers aucune classe de stockage.
- Les objets doivent être stockés pendant au moins 30 jours avant de passer à S3 Standard-IA ou S3 One Zone-IA.
- Pour le versionnement activé ou le versionnement des buckets suspendus, les objets dotés d'un statut de `PENDING` réplication ne peuvent pas être transférés.

Comment puis-je exclure un préfixe de ma règle de cycle de vie ?

S3 Lifecycle ne prend pas en charge l'exclusion des préfixes dans vos règles. Au lieu de cela, utilisez des balises pour baliser tous les objets que vous souhaitez inclure dans la règle. Pour plus d'informations sur l'utilisation de balises dans vos règles de cycle de vie, consultez the section called "Archivage de tous les objets dans un délai d'un jour après leur création".

Comment puis-je inclure plusieurs préfixes dans ma règle de cycle de vie ?

S3 Lifecycle ne prend pas en charge l'inclusion de plusieurs préfixes dans vos règles. Au lieu de cela, utilisez des balises pour baliser tous les objets que vous souhaitez inclure dans la règle. Pour plus d'informations sur l'utilisation de balises dans vos règles de cycle de vie, consultez the section called "Archivage de tous les objets dans un délai d'un jour après leur création".

Toutefois, si un ou plusieurs préfixes commencent par les mêmes caractères, vous pouvez inclure tous ces préfixes dans votre règle en spécifiant un préfixe partiel sans barre oblique (`/`) dans le filtre. Par exemple, supposons que vous avez les préfixes suivants :

```
sales1999/
```

```
sales2000/
sales2001/
```

Pour inclure ces trois préfixes dans votre règle, spécifiez `<Prefix>sales</Prefix>` dans votre règle de cycle de vie.

Journalisation et surveillance dans Amazon S3

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon S3 et de vos AWS solutions. Nous vous recommandons de collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une panne multipoint, le cas échéant. Avant de commencer à surveiller Amazon S3, créez un plan de surveillance qui comprend les réponses aux questions suivantes :

- Quels sont les objectifs de la surveillance ?
- Quelles sont les ressources à surveiller ?
- À quelle fréquence les ressources doivent-elles être surveillées ?
- Quels outils de surveillance utiliser ?
- Qui exécute les tâches de supervision ?
- Qui doit être informé en cas de problème ?

Pour en savoir plus sur la journalisation et la surveillance dans Amazon S3, consultez les rubriques suivantes.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité et des performances d'Amazon S3 et de vos AWS solutions. Vous devez collecter des données de surveillance provenant de toutes les parties de votre AWS solution afin de pouvoir corriger plus facilement une défaillance multipoint, le cas échéant. AWS fournit plusieurs outils pour surveiller vos ressources Amazon S3 et répondre aux incidents potentiels.

CloudWatch Alarmes Amazon

À l'aide des CloudWatch alarmes Amazon, vous observez une seule métrique sur une période que vous spécifiez. Si la métrique dépasse un seuil donné, une notification est envoyée à une rubrique ou AWS Auto Scaling à une politique Amazon SNS. CloudWatch les alarmes n'appellent

pas d'actions car elles se trouvent dans un état particulier. L'état doit avoir changé et avoir été conservé pendant un nombre de périodes spécifié. Pour de plus amples informations, veuillez consulter Surveillance des métriques avec Amazon CloudWatch.

AWS CloudTrail Journaux

CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon S3. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon S3, l'adresse IP à partir de laquelle la demande a été faite, l'auteur de la demande, la date à laquelle elle a été faite, ainsi que des informations supplémentaires. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail.

Amazon GuardDuty

Amazon GuardDuty est un service de détection des menaces qui surveille en permanence vos comptes, vos conteneurs, vos charges de travail et les données de votre AWS environnement afin d'identifier les menaces ou les risques de sécurité potentiels pour vos compartiments S3. GuardDuty fournit également un contexte détaillé sur les menaces détectées. GuardDuty surveille les journaux AWS CloudTrail de gestion pour détecter les menaces et affiche les informations relatives à la sécurité. Par exemple, GuardDuty inclura les facteurs d'une demande d'API, tels que l'utilisateur qui a fait la demande, le lieu d'où la demande a été faite et l'API spécifique demandée, qui peuvent être inhabituels dans votre environnement. GuardDuty S3 Protection surveille les événements de données S3 collectés par CloudTrail et identifie les comportements potentiellement anormaux et malveillants dans tous les compartiments S3 de votre environnement.

Journaux d'accès Amazon S3

Les journaux d'accès au serveur fournissent des enregistrements détaillés sur les demandes formulées à un compartiment. Les journaux d'accès au serveur sont utiles pour de nombreuses applications. Par exemple, les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Pour de plus amples informations, veuillez consulter Enregistrement de demandes avec journalisation des accès au serveur.

AWS Trusted Advisor

Trusted Advisor s'appuie sur les meilleures pratiques apprises en servant des centaines de milliers de AWS clients. Trusted Advisor inspecte votre AWS environnement, puis émet des recommandations lorsque des opportunités se présentent pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité.

Tous les AWS clients ont accès à cinq Trusted Advisor chèques. Les clients disposant d'un plan de support Business ou Enterprise peuvent consulter tous les Trusted Advisor chèques.

Trusted Advisor comporte les vérifications suivantes relatives à Amazon S3 :

- Configuration de journalisation des compartiments Amazon S3.
- Contrôles de sécurité pour les compartiments Amazon S3 dont les autorisations permettent un libre accès.
- Vérifications de la tolérance aux pannes pour les compartiments Amazon S3 pour lesquels la gestion des versions est désactivée ou suspendue.

Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur Support .

Amazon S3 Storage Lens

Amazon S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Vous pouvez utiliser les métriques S3 Storage Lens pour générer des informations récapitulatives, telles que la quantité de stockage dont vous disposez dans l'ensemble de votre organisation ou les compartiments et préfixes qui connaissent la croissance la plus rapide. Vous pouvez également utiliser les métriques S3 Storage Lens pour identifier les opportunités d'optimisation des coûts, mettre en œuvre les bonnes pratiques de protection et de sécurisation des données et améliorer les performances des charges de travail d'application.

S3 Storage Lens regroupe vos métriques et affiche les informations dans la section Instantané du compte sur la page Compartiments de la console Amazon S3. S3 Storage Lens fournit également un tableau de bord interactif que vous pouvez utiliser pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord comporte des options d'exploration permettant de générer et de visualiser des informations au niveau de l'organisation, du compte, de la classe de stockage Région AWS, du bucket, du préfixe ou du groupe Storage Lens. Pour de plus amples informations, veuillez consulter Présentation d'Amazon S3 Storage Lens.

Inventaire Amazon S3

L'inventaire Amazon S3 génère une liste d'objets et de métadonnées que vous pouvez utiliser pour interroger et gérer vos objets. Vous pouvez utiliser ce rapport d'inventaire pour générer des données granulaires telles que la taille de l'objet, la date de dernière modification, le statut du chiffrement et d'autres champs. Ces rapports sont disponibles à une fréquence quotidienne ou hebdomadaire pour fournir automatiquement la dernière liste.

Par exemple, vous pouvez utiliser l'inventaire Amazon S3 pour auditer et signaler le statut de réplication et de chiffrement de vos objets à des fins de gestion, de conformité et d'obligations réglementaires. Vous pouvez également utiliser l'inventaire Amazon S3 pour simplifier et accélérer les flux de travail métier et les tâches du big data, ce qui fournit une alternative planifiée aux opérations d'API `List` synchrones Amazon S3. L'inventaire Amazon S3 n'utilise pas les opérations d'API `List` pour auditer vos objets et n'affecte pas le taux de demande de votre compartiment. Pour de plus amples informations, veuillez consulter Catalogage et analyse de vos données avec l'inventaire S3.

Notifications d'événements Amazon S3

Avec la fonctionnalité Notifications d'événements Amazon S3, vous recevez des notifications lorsque certains événements se produisent dans votre compartiment S3. Pour activer les notifications, ajoutez une configuration de notification qui identifie les événements que Amazon S3 doit publier. Pour de plus amples informations, veuillez consulter Notifications d'événements Amazon S3.

Amazon S3 et AWS X-Ray

AWS X-Ray s'intègre à Amazon S3 pour suivre les demandes en amont visant à mettre à jour les compartiments S3 de votre application. Si un service effectue le suivi des demandes à l'aide du kit SDK X-Ray, Amazon S3 peut envoyer les en-têtes de suivi aux abonnés aux événements en aval, comme Λ, Amazon SQS et Amazon SNS. X-Ray active les messages de suivi pour les notifications d'événements Amazon S3. Vous pouvez utiliser la carte de suivi X-Ray pour afficher les connexions entre Amazon S3 et les autres services que votre application utilise. Pour plus d'informations, consultez Amazon S3 et X-Ray.

Les bonnes pratiques de sécurité suivantes s'appliquent également à la consignation et à la surveillance :

- Identify and audit all your Amazon S3 buckets
- Implement monitoring using Amazon Web Services monitoring tools
- Activer AWS Config
- Enable Amazon S3 server access logging
- Use CloudTrail
- Monitor Amazon Web Services security advisories

Rubriques

- Outils de surveillance
- Options de journalisation pour Amazon S3
- Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail
- Enregistrement de demandes avec journalisation des accès au serveur
- Surveillance des métriques avec Amazon CloudWatch
- Notifications d'événements Amazon S3
- Évaluer l'activité et l'utilisation de votre stockage avec Amazon S3 Storage Lens
- Catalogage et analyse de vos données avec l'inventaire S3

Outils de surveillance

AWS fournit différents outils que vous pouvez utiliser pour surveiller Amazon S3. Vous pouvez configurer certains outils pour qu'ils effectuent la supervision automatiquement, tandis que d'autres nécessitent une intervention manuelle. Nous vous recommandons d'automatiser le plus possible les tâches de supervision.

Outils de surveillance automatique

Vous pouvez utiliser les outils de surveillance automatique pour surveiller Amazon S3 et signaler un problème éventuel :

- Amazon CloudWatch Alarms — Surveillez une seule métrique sur une période que vous spécifiez et effectuez une ou plusieurs actions en fonction de la valeur de la métrique par rapport à un seuil donné sur un certain nombre de périodes. L'action est une notification envoyée à une rubrique Amazon Simple Notification Service (Amazon SNS) ou à une politique Amazon EC2 Auto Scaling. CloudWatch les alarmes n'appellent pas d'actions simplement parce qu'elles sont dans un état particulier. L'état doit avoir changé et avoir été maintenu pendant un nombre de périodes spécifié. Pour de plus amples informations, veuillez consulter Surveillance des métriques avec Amazon CloudWatch.
- AWS CloudTrail Surveillance des journaux : partagez les fichiers journaux entre les comptes, surveillez les fichiers CloudTrail CloudWatch journaux en temps réel en les envoyant à Logs, écrivez des applications de traitement des journaux en Java et vérifiez que vos fichiers journaux n'ont pas changé après leur livraison par CloudTrail. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail.

Outils de surveillance manuelle

Un autre aspect important de la surveillance d'Amazon S3 consiste à surveiller manuellement les éléments non couverts par les CloudWatch alarmes. Les AWS Management Console tableaux de bord Amazon S3 CloudWatch Trusted Advisor,,, et d'autres fournissent une at-a-glance vue de l'état de votre AWS environnement. Vous pouvez activer la journalisation des accès au serveur pour suivre les demandes d'accès à votre compartiment. Chaque enregistrement de journal d'accès fournit des informations détaillées sur une demande d'accès donnée (demandeur, nom du compartiment, heure de la demande, action associée à la demande, état de la réponse et code d'erreur, le cas échéant). Pour plus d'informations, consultez Enregistrement de demandes avec journalisation des accès au serveur.

- Le tableau de bord Amazon S3 affiche les éléments suivants :
  - Vos compartiments et les objets et propriétés qu'ils contiennent
- La page CloudWatch d'accueil affiche les informations suivantes :
  - Alarmes et statuts en cours
  - Graphiques des alarmes et des ressources
  - Statut d'intégrité du service

  En outre, vous pouvez utiliser CloudWatch pour effectuer les opérations suivantes :
  - Créer des tableaux de bord personnalisés pour surveiller les services de votre choix.
  - Données de métriques de graphiques pour résoudre les problèmes et découvrir les tendances.
  - Recherchez et parcourez tous les indicateurs de vos AWS ressources.
  - Créer et Modifier des alarmes pour être informé des problèmes.
- AWS Trusted Advisor peut vous aider à surveiller vos AWS ressources afin d'améliorer les performances, la fiabilité, la sécurité et la rentabilité. Quatre contrôles Trusted Advisor sont disponibles pour tous les utilisateurs. Plus de 50 contrôles sont disponibles pour les utilisateurs avec un plan de support Business ou Enterprise. Pour de plus amples informations, veuillez consulter AWS Trusted Advisor.

  Trusted Advisor possède les vérifications suivantes relatives à Amazon S3 :
  - Vérification de la configuration de journalisation des compartiments Amazon S3.
  - Vérifications de sécurité pour les compartiments Amazon S3 dont les autorisations permettent un libre accès.

- Vérifications de la tolérance aux pannes pour les compartiments Amazon S3 pour lesquels la gestion des versions est désactivée ou suspendue.

Options de journalisation pour Amazon S3

Vous pouvez enregistrer les actions entreprises par les utilisateurs, les rôles ou Services AWS sur les ressources Amazon S3 et conserver des enregistrements de journal à des fins d'audit et de conformité. Pour ce faire, vous pouvez utiliser la journalisation d'accès au serveur, la journalisation AWS CloudTrail ou une combinaison des deux. Nous vous recommandons de l'utiliser CloudTrail pour consigner les actions au niveau du bucket et au niveau de l'objet pour vos ressources Amazon S3. Pour plus d'informations, consultez les sections suivantes :

- Enregistrement de demandes avec journalisation des accès au serveur
- Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail

Le tableau suivant répertorie les principales propriétés des CloudTrail journaux et des journaux d'accès au serveur Amazon S3. Pour vous assurer que cela CloudTrail répond à vos exigences de sécurité, consultez le tableau et les notes.

Propriétés des journaux	AWS CloudTrail	Journaux du serveur Amazon S3
Peut être transféré vers d'autres systèmes (Amazon CloudWatch Logs, Amazon CloudWatch Events)	Oui	Non
Acheminement des journaux vers plusieurs destinations (par exemple, envoi des mêmes journaux vers deux compartiments différents).	Oui	Non
Activation des journaux sur un sous-ensemble d'objets (préfixe)	Oui	Non

Propriétés des journaux	AWS CloudTrail	Journaux du serveur Amazon S3
Fourniture de journaux inter-comptes (compartiments cible et source appartenant à des comptes différents)	Oui	Non
Validation de l'intégrité du fichier journal en utilisant la signature numérique ou le hachage.	Oui	Non
Choix ou défaut de chiffrement pour les fichiers journaux.	Oui	Non
Opérations sur les objets (à l'aide d'Amazon S3 APIs)	Oui	Oui
Opérations sur les compartiments (à l'aide d'Amazon S3 APIs)	Oui	Oui
Interface utilisateur pouvant faire l'objet d'une recherche sur les journaux	Oui	Non
Champs pour les paramètres de verrouillage des objets Object Lock, propriétés de sélection Amazon S3 Select pour les enregistrements de journaux	Oui	Non

Propriétés des journaux	AWS CloudTrail	Journaux du serveur Amazon S3
Champs pour `Object Size`, `Total Time`, `Turn-Around Time` et `HTTP Referer` pour les enregistrements de journaux	Non	Oui
Restaurations, expirations et transitions de cycle de vie	Non	Oui
Consignation des clés dans une opération d'effacement par batchs	Oui	Oui
Échecs d'authentification[1]	Non	Oui
Comptes où les journaux ont été livrés	Propriétaire du compartiment[2] et demandeur	Propriétaire du compartiment uniquement
Performance and Cost	AWS CloudTrail	Amazon S3 Server Logs
Prix	Les événements de gestion (première livraison) sont gratuits ; les événements de données sont payants, en plus du stockage des journaux.	Aucun autre coût en plus du stockage des journaux
Rapidité de fourniture des journaux	Événements de données toutes les 5 minutes ; événements de gestion toutes les 15 minutes	Sous quelques heures
Format des journaux	JSON	Fichier journal avec enregistrements séparés par des espaces, délimités par de nouvelles lignes

Remarques

1. CloudTrail ne fournit pas de journaux pour les demandes qui échouent à l'authentification (pour lesquelles les informations d'identification fournies ne sont pas valides) ou qui échouent en raison d'une redirection (code d'erreur`301 Moved Permanently`). Cependant, sont fournis les journaux pour les requêtes dans lesquelles l'autorisation a échoué (`AccessDenied`) et les demandes formulées par des utilisateurs anonymes.
2. Le propriétaire du compartiment S3 reçoit CloudTrail des journaux lorsque le compte ne dispose pas d'un accès complet à l'objet figurant dans la demande. Pour de plus amples informations, veuillez consulter Actions au niveau des objets Amazon S3 dans les scénarios intercomptes.
3. S3 ne prend pas en charge la livraison de CloudTrail journaux ou de journaux d'accès au serveur au demandeur ou au propriétaire du compartiment pour les demandes de point de terminaison VPC lorsque la politique de point de terminaison du VPC les refuse ou pour les demandes qui échouent avant que la politique VPC ne soit évaluée.

Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail

Amazon S3 est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API pour Amazon S3 sous forme d'événements. Ces captures incluent les appels de la console Amazon S3 et les appels de code vers les opérations d'API Amazon S3. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande envoyée à Amazon S3, 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 CloudTrail Lake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console 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 d'exécuter des requêtes SQL 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.

Vous pouvez stocker vos fichiers journaux dans votre compartiment aussi longtemps que vous le souhaitez, ou bien définir des règles de cycle de vie Amazon S3 afin de les archiver ou de les supprimer automatiquement. Par défaut, vos fichiers journaux sont chiffrés à l'aide du chiffrement côté serveur (SSE) d'Amazon S3.

Utilisation de CloudTrail journaux avec les journaux d'accès au serveur Amazon S3 et CloudWatch les journaux

AWS CloudTrail les journaux fournissent un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Amazon S3, tandis que les journaux d'accès au serveur Amazon S3 fournissent des enregistrements détaillés des demandes adressées à un compartiment S3. Pour plus d'informations sur le fonctionnement des différents journaux ainsi que sur leurs propriétés, performances et coûts, consultez the section called "Options de journalisation".

Vous pouvez utiliser AWS CloudTrail les journaux avec les journaux d'accès au serveur pour Amazon S3. CloudTrail les journaux vous fournissent un suivi détaillé des API pour les opérations au niveau du bucket et au niveau de l'objet d'Amazon S3. Les journaux d'accès au serveur pour Amazon S3 vous donnent la visibilité nécessaire sur les opérations d'objet au niveau de vos données dans Amazon S3. Pour plus d'informations sur les journaux d'accès au serveur, consultez Enregistrement de demandes avec journalisation des accès au serveur.

Vous pouvez également utiliser CloudTrail les journaux avec Amazon CloudWatch pour Amazon S3. CloudTrail l'intégration avec CloudWatch Logs fournit l'activité de l'API au niveau du compartiment S3 capturée par CloudTrail un flux de CloudWatch journaux dans le groupe de CloudWatch journaux que vous spécifiez. Vous pouvez créer des CloudWatch alarmes pour surveiller une activité d'API spécifique et recevoir des notifications par e-mail lorsque l'activité d'API spécifique se produit. Pour plus d'informations sur les CloudWatch alarmes destinées à surveiller une activité d'API

spécifique, consultez le guide de AWS CloudTrail l'utilisateur. Pour plus d'informations sur l'utilisation CloudWatch avec Amazon S3, consultezSurveillance des métriques avec Amazon CloudWatch.

> **Note**
>
> S3 ne prend pas en charge la remise de CloudTrail journaux au demandeur ou au propriétaire du compartiment pour les demandes de point de terminaison VPC lorsque la politique de point de terminaison du VPC les refuse.

CloudTrail suivi avec les appels d'API SOAP Amazon S3

CloudTrail suit les appels d'API SOAP Amazon S3. La prise en charge de SOAP par Amazon S3 via HTTP est obsolète, mais continue d'être disponible via HTTPS. Pour plus d'informations sur la prise en charge d'Amazon S3 SOAP, consultez Annexe : API SOAP dans la Référence d'API Amazon S3.

> **Important**
>
> Les nouvelles fonctions Amazon S3 ne sont pas prises en charge pour SOAP. Nous vous recommandons d'utiliser l'API REST ou le AWS SDKs.

Le tableau suivant présente les actions SOAP Amazon S3 suivies par CloudTrail journalisation.

Nom d'API SOAP	Nom de l'événement API utilisé dans le CloudTrail journal
ListAllMyBuckets	`ListBuckets`
CreateBucket	`CreateBucket`
DeleteBucket	`DeleteBucket`
GetBucketAccessControlPolicy	`GetBucketAcl`
SetBucketAccessControlPolicy	`PutBucketAcl`
GetBucketLoggingStatus	`GetBucketLogging`

Nom d'API SOAP	Nom de l'événement API utilisé dans le CloudTrail journal
SetBucketLoggingStatus	`PutBucketLogging`

Pour plus d'informations sur Amazon S3 CloudTrail et Amazon S3, consultez les rubriques suivantes :

Rubriques

- CloudTrail Événements Amazon S3
- CloudTrail entrées de fichiers journaux pour Amazon S3 et S3 on Outposts
- Activation de la journalisation des CloudTrail événements pour les compartiments et les objets S3
- Identification des demandes Amazon S3 à l'aide de CloudTrail

CloudTrail Événements Amazon S3

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Cette section fournit des informations sur les événements auxquels S3 se connecte CloudTrail.

Événements liés aux données Amazon S3 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 dont le volume est élevé. Par défaut, CloudTrail n'enregistre pas les événements liés aux données. L'historique des CloudTrail événements n'enregistre pas les événements liés aux données.

Des frais supplémentaires s'appliquent pour les événements de données. Pour plus d'informations sur la tarification CloudTrail, consultez Tarification AWS CloudTrail.

Vous pouvez enregistrer les événements de données pour les types de ressources Amazon S3 à l'aide de la CloudTrail console ou des opérations CloudTrail d'API. AWS CLI Pour plus d'informations sur la façon de journaliser les événements de données, consultez Journalisation des événements de données avec la AWS Management Console 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 Amazon S3 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 du ou. AWS CLI CloudTrail APIs La CloudTrail colonne Données APIs enregistrées indique les appels d'API enregistrés CloudTrail pour le type de ressource.

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
S3	`AWS::S3::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • DeleteObjects • GetObject • GetObjectAcl • GetObjectAttributes

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
		• GetObjectLegalHold • GetObjectRetention • GetObjectTagging • GetObjectTorrent • HeadObject • HeadBucket • ListObjectVersions • ListObjects • ListParts • PutObject • PutObjectAcl • PutObjectLegalHold • PutObjectRetention • PutObjectTagging • RestoreObject • SelectObjectContent • UploadPart • UploadPartCopy

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
S3 Express One Zone	`AWS::S3Express::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CreateSession • CopyObject • CreateMultipartUpload • DeleteObject • DeleteObjects • GetObject • GetObjectAttributes • HeadBucket • HeadObject • ListObjectsV2 • ListParts • PutObject • UploadPart • UploadPartCopy

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
Points d'accès S3	`AWS::S3::Access Point`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (copies dans une même Région uniquement) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetBucketAcl • GetBucketCors • GetBucketLocation • GetBucketNotificationConfiguration • GetBucketPolicy • GetObject • GetObjectAcl • GetObjectAttributes • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • HeadBucket • HeadObject • ListObjects • ListObjectsV2 • ListObjectVersions • ListParts • Presign • PutObject

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
		• PutObjectLegalHold • PutObjectRetention • PutObjectAcl • PutObjectTagging • RestoreObject • UploadPart • UploadPartCopy (copies dans une même Région uniquement)

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
S3 Object Lambda	`AWS::S3ObjectLambda::AccessPoint`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (copies dans une même Région uniquement) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectAcl • GetObjectLegalHold • GetObjectRetention • GetObjectTagging • HeadObject • ListObjects • ListObjectVersions • ListParts • PutObject • PutObjectLegalHold • PutObjectRetention • PutObjectAcl • PutObjectTagging • RestoreObject • UploadPart • WriteGetObjectResponse

Type d'événement de données (console)	valeur resources.type	Données APIs enregistrées sur CloudTrail
S3 Outposts	`AWS::S3Outposts::Object`	• AbortMultipartUpload • CompleteMultipartUpload • CopyObject (copies dans une même Région uniquement) • CreateMultipartUpload • DeleteObject • DeleteObjectTagging • GetObject • GetObjectTagging • HeadObject • ListObjects • ListObjectsV2 • ListParts • PutObject • PutObjectTagging • UploadPart • UploadPartCopy

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. Pour plus d'informations sur ces champs, consultez AdvancedFieldSelector dans la Référence d'API AWS CloudTrail .

Événements de gestion Amazon S3 dans CloudTrail

Amazon S3 journalise toutes les opérations du plan de contrôle en tant qu'événements de gestion. Pour plus d'informations sur les opérations d'API S3, consultez Référence d'API Amazon S3.

Comment CloudTrail capture les demandes adressées à Amazon S3

Par défaut, CloudTrail enregistre les appels d'API au niveau du compartiment S3 effectués au cours des 90 derniers jours, mais pas les demandes de journalisation adressées aux objets. Les appels au niveau des compartiments comprennent des événements tels que `CreateBucket`, `DeleteBucket`, `PutBucketLifecycle`, `PutBucketPolicy` et ainsi de suite. Vous pouvez voir les événements au niveau du bucket sur la CloudTrail console. Cependant, vous ne pouvez pas y consulter les événements de données (appels au niveau des objets Amazon S3). Vous devez les analyser ou les consulter dans les journaux. CloudTrail

Si vous enregistrez une activité liée aux données avec AWS CloudTrail, l'enregistrement d'un événement de `DeleteObjects` données Amazon S3 inclut à la fois l'`DeleteObjects`événement et un `DeleteObject` événement pour chaque objet supprimé dans le cadre de cette opération. Vous pouvez exclure de l'enregistrement d'événements la visibilité supplémentaire sur les objets supprimés. Pour plus d'informations, consultez les AWS CLI exemples de filtrage des événements de données dans le Guide de AWS CloudTrail l'utilisateur.

Actions au niveau du compte Amazon S3 suivies par journalisation CloudTrail

CloudTrail enregistre les actions au niveau du compte. Les enregistrements Amazon S3 sont écrits avec d'autres Service AWS enregistrements dans un fichier journal. CloudTrail détermine à quel moment créer et écrire dans un nouveau fichier en fonction d'une période et de la taille du fichier.

Les tableaux de cette section répertorient les actions au niveau du compte Amazon S3 prises en charge pour la connexion par. CloudTrail

Les actions d'API au niveau du compte Amazon S3 suivies par CloudTrail journalisation apparaissent sous les noms d'événements suivants. Les noms des CloudTrail événements sont différents du nom de l'action de l'API. Par exemple, DeletePublicAccessBlock est DeleteAccountPublicAccessBlock.

- DeleteAccountPublicAccessBlock
- GetAccountPublicAccessBlock
- PutAccountPublicAccessBlock

Actions au niveau du compartiment Amazon S3 suivies par journalisation CloudTrail

Par défaut, CloudTrail enregistre les actions au niveau du compartiment pour les compartiments à usage général. Les enregistrements Amazon S3 sont écrits avec d'autres enregistrements AWS de

service dans un fichier journal. CloudTrail détermine à quel moment créer et écrire dans un nouveau fichier en fonction d'une période et de la taille du fichier.

Cette section répertorie les actions au niveau du compartiment Amazon S3 prises en charge pour la journalisation. CloudTrail

Les actions d'API au niveau du bucket Amazon S3 suivies par CloudTrail journalisation apparaissent sous les noms d'événements suivants. Dans certains cas, le nom de l' CloudTrail événement est différent du nom de l'action de l'API. Par exemple, `PutBucketLifecycleConfiguration` est `PutBucketLifecycle`.

- CreateBucket
- CreateBucketMetadataConfiguration(fonctionnement de l'API V2)
- CreateBucketMetadataTableConfiguration(fonctionnement de l'API V1)
- DeleteBucket
- DeleteBucketAnalyticsConfiguration
- DeleteBucketCors
- DeleteBucketEncryption
- DeleteBucketIntelligentTieringConfiguration
- DeleteBucketInventoryConfiguration
- DeleteBucketLifecycle
- DeleteBucketMetadataConfiguration(fonctionnement de l'API V2)
- DeleteBucketMetadataTableConfiguration(fonctionnement de l'API V1)
- DeleteBucketMetricsConfiguration
- DeleteBucketOwnershipControls
- DeleteBucketPolicy
- DeleteBucketPublicAccessBlock
- DeleteBucketReplication
- DeleteBucketTagging
- GetAccelerateConfiguration
- GetBucketAcl
- GetBucketAnalyticsConfiguration

- GetBucketCors
- GetBucketEncryption
- GetBucketIntelligentTieringConfiguration
- GetBucketInventoryConfiguration
- GetBucketLifecycle
- GetBucketLocation
- GetBucketLogging
- GetBucketMetadataConfiguration(fonctionnement de l'API V2)
- GetBucketMetadataTableConfiguration(fonctionnement de l'API V1)
- GetBucketMetricsConfiguration
- GetBucketNotification
- GetBucketObjectLockConfiguration
- GetBucketOwnershipControls
- GetBucketPolicy
- GetBucketPolicyStatus
- GetBucketPublicAccessBlock
- GetBucketReplication
- GetBucketRequestPayment
- GetBucketTagging
- GetBucketVersioning
- GetBucketWebsite
- HeadBucket
- ListBuckets
- PutAccelerateConfiguration
- PutBucketAcl
- PutBucketAnalyticsConfiguration
- PutBucketCors
- PutBucketEncryption
- PutBucketIntelligentTieringConfiguration

- PutBucketInventoryConfiguration
- PutBucketLifecycle
- PutBucketLogging
- PutBucketMetricsConfiguration
- PutBucketNotification
- PutBucketObjectLockConfiguration
- PutBucketOwnershipControls
- PutBucketPolicy
- PutBucketPublicAccessBlock
- PutBucketReplication
- PutBucketRequestPayment
- PutBucketTagging
- PutBucketVersioning
- PutBucketWebsite
- UpdateBucketMetadataJournalTableConfiguration
- UpdateBucketMetadataInventoryTableConfiguration

En plus de ces opérations d'API, vous pouvez également utiliser l'action au niveau de l'objet OPTIONS object. Cette action est traitée comme une action au niveau du compartiment dans la CloudTrail journalisation, car elle vérifie la configuration CORS d'un compartiment.

Actions Amazon S3 Express One Zone au niveau du bucket (point de terminaison d'API régional) suivies par journalisation CloudTrail

Par défaut, CloudTrail enregistre les actions au niveau du compartiment pour les compartiments de répertoire en tant qu'événements de gestion. Les événements CloudTrail de gestion `eventsource` pour S3 Express One Zone sont`s3express.amazonaws.com`.

Les opérations suivantes de l'API de point de terminaison régional sont enregistrées sur CloudTrail.

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy

- GetBucketPolicy
- PutBucketPolicy
- ListDirectoryBuckets
- PutBucketEncryption
- GetBucketEncryption
- DeleteBucketEncryption

Pour plus d'informations, voir Logging with AWS CloudTrail for S3 Express One Zone

Actions au niveau des objets Amazon S3 dans les scénarios intercomptes

Vous trouverez ci-dessous des cas d'utilisation particuliers impliquant les appels d'API au niveau de l'objet dans des scénarios entre comptes et la manière dont les CloudTrail journaux sont signalés. CloudTrail fournit les journaux au demandeur (le compte qui a effectué l'appel d'API), sauf dans certains cas de refus d'accès où les entrées du journal sont expurgées ou omises. Lorsque vous configurez l'accès intercompte, pensez aux exemples de cette section.

> **Note**
>
> Les exemples supposent que CloudTrail les journaux sont correctement configurés.

Exemple 1 : CloudTrail fournit des journaux au propriétaire du compartiment

CloudTrail fournit des journaux au propriétaire du compartiment même si celui-ci n'est pas autorisé à effectuer la même opération d'API d'objet. Envisagez le scénario entre comptes suivant :

- Le compte A est le propriétaire du compartiment.
- Le compte B (le demandeur) tente d'accéder à un objet de ce compartiment.
- Le compte C est propriétaire de l'objet. Le compte C peut ou non être le même compte que le compte A.

> **Note**
>
> CloudTrail fournit toujours des journaux d'API au niveau de l'objet au demandeur (compte B). En outre, fournit CloudTrail également les mêmes journaux au propriétaire du bucket

(compte A) même si celui-ci n'est pas propriétaire de l'objet (compte C) ou n'est pas autorisé à effectuer les mêmes opérations d'API sur cet objet.

Exemple 2 : CloudTrail ne multiplie pas les adresses e-mail utilisées pour définir l'objet ACLs

Envisagez le scénario entre comptes suivant :

- Le compte A est le propriétaire du compartiment.
- Le compte B (le demandeur) envoie une demande pour définir un octroi de liste ACL d'objet en utilisant une adresse e-mail. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL).

Le demandeur obtient les journaux ainsi que les informations de messagerie. Toutefois, le propriétaire du compartiment, s'il est éligible pour recevoir des journaux, comme dans l'exemple, obtient que le CloudTrail journal signale l'événement. Cependant, le propriétaire du compartiment n'obtient pas les informations de configuration de liste ACL, notamment l'adresse e-mail du bénéficiaire et l'octroi. La seule information transmise par le journal au propriétaire du compartiment est qu'un appel d'API de liste ACL a été passé par le compte B.

CloudTrail entrées de fichiers journaux pour Amazon S3 et S3 on Outposts

Important

Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

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.

> **Note**
>
> Pour consulter des exemples de fichiers CloudTrail journaux pour Amazon S3 Express One Zone, consultez les exemples de fichiers CloudTrail journaux pour S3 Express One Zone.

Pour plus d'informations, consultez les exemples suivants.

Rubriques

- Exemple : entrée de fichier CloudTrail journal pour Amazon S3

Exemple : entrée de fichier CloudTrail journal pour Amazon S3

L'exemple suivant montre une entrée de CloudTrail journal illustrant le GETservice et PutBucketAcllesGetBucketVersioningactions.


```
{
    "Records": [
    {
        "eventVersion": "1.03",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2019-02-01T03:18:19Z",
        "eventSource": "s3.amazonaws.com",
        "eventName": "ListBuckets",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "host": [
                "s3.us-west-2.amazonaws.com"
            ]
```

```
        },
        "responseElements": null,
        "additionalEventData": {
            "SignatureVersion": "SigV2",
            "AuthenticationMethod": "QueryString",
            "aclRequired": "Yes"
    },
        "requestID": "47B8E8D397DCE7A6",
        "eventID": "cdc4b7ed-e171-4cef-975a-ad829d4123e8",
        "eventType": "AwsApiCall",
        "recipientAccountId": "444455556666",
        "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.amazonaws.com"
    }
    },
    {
       "eventVersion": "1.03",
       "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
      "eventTime": "2019-02-01T03:22:33Z",
      "eventSource": "s3.amazonaws.com",
      "eventName": "PutBucketAcl",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "",
      "userAgent": "[]",
      "requestParameters": {
          "bucketName": "",
          "AccessControlPolicy": {
              "AccessControlList": {
                  "Grant": {
                      "Grantee": {
                          "xsi:type": "CanonicalUser",
                          "xmlns:xsi": "http://www.w3.org/2001/XMLSchema-instance",
                          "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
                       },
```

```
                    "Permission": "FULL_CONTROL"
                }
            },
            "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/",
            "Owner": {
                "ID":
"d25639fbe9c19cd30a4c0f43fbf00e2d3f96400a9aa8dabfbbebe1906Example"
            }
        },
        "host": [
            "s3.us-west-2.amazonaws.com"
        ],
        "acl": [
            ""
        ]
    },
    "responseElements": null,
    "additionalEventData": {
        "SignatureVersion": "SigV4",
        "CipherSuite": "ECDHE-RSA-AES128-SHA",
        "AuthenticationMethod": "AuthHeader"
    },
    "requestID": "BD8798EACDD16751",
    "eventID": "607b9532-1423-41c7-b048-ec2641693c47",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333",
    "tlsDetails": {
          "tlsVersion": "TLSv1.2",
          "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
          "clientProvidedHostHeader": "s3.amazonaws.com"
  }
  },
  {
    "eventVersion": "1.03",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "111122223333",
        "arn": "arn:aws:iam::111122223333:user/myUserName",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "userName": "myUserName"
      },
    "eventTime": "2019-02-01T03:26:37Z",
    "eventSource": "s3.amazonaws.com",
```

```
      "eventName": "GetBucketVersioning",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "",
      "userAgent": "[]",
      "requestParameters": {
          "host": [
              "s3.us-west-2.amazonaws.com"
          ],
          "bucketName": "amzn-s3-demo-bucket1",
          "versioning": [
              ""
          ]
      },
      "responseElements": null,
      "additionalEventData": {
          "SignatureVersion": "SigV4",
          "CipherSuite": "ECDHE-RSA-AES128-SHA",
          "AuthenticationMethod": "AuthHeader"
    },
      "requestID": "07D681279BD94AED",
      "eventID": "f2b287f3-0df1-4961-a2f4-c4bdfed47657",
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333",
      "tlsDetails": {
            "tlsVersion": "TLSv1.2",
            "cipherSuite": "ECDHE-RSA-AES128-GCM-SHA256",
            "clientProvidedHostHeader": "s3.amazonaws.com"
    }
    }
  ]
}
```

Activation de la journalisation des CloudTrail événements pour les compartiments et les objets S3

Vous pouvez utiliser CloudTrail les événements de données pour obtenir des informations sur les requêtes au niveau du compartiment et de l'objet dans Amazon S3. Pour activer les événements de CloudTrail données pour tous vos compartiments ou pour une liste de compartiments spécifiques, vous devez créer un suivi manuellement dans. CloudTrail

> **Note**
>
> - Le paramètre par défaut pour CloudTrail est de rechercher uniquement les événements de gestion. Assurez-vous que vous avez activé les événements de données pour votre compte.
> - Avec un compartiment S3 qui génère une charge de travail élevée, vous pourriez rapidement générer des milliers de journaux en un temps très court. Tenez compte de la durée pendant laquelle vous choisissez d'activer CloudTrail les événements de données pour un compartiment occupé.

CloudTrail stocke les journaux d'événements de données Amazon S3 dans un compartiment S3 de votre choix. Envisagez d'utiliser un compartiment séparé Compte AWS pour mieux organiser les événements provenant de plusieurs compartiments que vous pourriez posséder dans un emplacement central afin de faciliter les requêtes et les analyses. AWS Organizations vous permet de créer un Compte AWS compte lié au compte propriétaire du bucket que vous surveillez. Pour plus d'informations, voir Qu'est-ce que c'est AWS Organizations ? dans le guide de AWS Organizations l'utilisateur.

Lorsque vous enregistrez des événements de données pour un trail in CloudTrail, vous pouvez choisir d'utiliser des sélecteurs d'événements avancés ou des sélecteurs d'événements de base pour enregistrer les événements de données relatifs aux objets stockés dans des compartiments à usage général. Pour journaliser des événements de données pour des objets stockés dans des compartiments de répertoires, vous devez utiliser des sélecteurs d'événements avancés. Pour plus d'informations, consultez Logging with AWS CloudTrail for S3 Express One Zone.

Lorsque vous créez un suivi dans la CloudTrail console à l'aide de sélecteurs d'événements avancés, dans la section Événements de données, vous pouvez sélectionner Enregistrer tous les événements pour que le modèle de sélecteur de journal enregistre tous les événements au niveau de l'objet. Lorsque vous créez un suivi dans la CloudTrail console à l'aide de sélecteurs d'événements de base, dans la section des événements de données, vous pouvez cocher la case Sélectionner tous les compartiments S3 de votre compte pour consigner tous les événements au niveau de l'objet.

> **Note**
>
> - Il est recommandé de créer une configuration de cycle de vie pour votre compartiment d'événements de données AWS CloudTrail . Configurez la configuration de cycle de vie

pour supprimer périodiquement les fichiers journaux après le délai à l'issue duquel vous estimez devoir les auditer. Cela permet de réduire la quantité de données analysées par Athena pour chaque requête. Pour plus d'informations, consultez Définition d'une configuration du cycle de vie S3 sur un compartiment.

- Pour plus d'informations sur le format de la journalisation, consultez Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail.
- Pour des exemples expliquant comment interroger les CloudTrail journaux, consultez le billet de blog AWS consacré au Big Data Analyze Security, Compliance, and Operational Activity Using AWS CloudTrail et Amazon Athena.

Activer la journalisation des objets d'un compartiment à l'aide de la console

Vous pouvez utiliser la console Amazon S3 pour configurer un AWS CloudTrail suivi afin de consigner les événements de données relatifs aux objets d'un compartiment S3. CloudTrail prend en charge la journalisation des opérations d'API au niveau des objets Amazon S3`GetObject`, telles que`DeleteObject`, et. `PutObject` Ces événements sont des événements de données.

Par défaut, les CloudTrail sentiers n'enregistrent pas les événements de données, mais vous pouvez configurer les sentiers pour enregistrer les événements de données pour les compartiments S3 que vous spécifiez, ou pour enregistrer les événements de données pour tous les compartiments Amazon S3 de votre. Compte AWS Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail.

CloudTrail ne renseigne pas les événements de données dans l'historique des CloudTrail événements. De plus, les actions au niveau du bucket ne sont pas toutes renseignées dans l'historique des CloudTrail événements. Pour plus d'informations sur les actions d'API au niveau du bucket Amazon S3 suivies par CloudTrail journalisation, consultez. Actions au niveau du compartiment Amazon S3 suivies par journalisation CloudTrail Pour plus d'informations sur la manière d'interroger CloudTrail les journaux, consultez l'article du centre de AWS connaissances sur l'utilisation des modèles de filtre Amazon CloudWatch Logs et d'Amazon Athena pour interroger CloudTrail les journaux.

> **Note**
>
> Si vous enregistrez une activité liée aux données avec AWS CloudTrail, l'enregistrement d'un événement de `DeleteObjects` données Amazon S3 inclut à la fois l'`DeleteObjects`événement et un `DeleteObject` événement pour chaque objet supprimé

dans le cadre de cette opération. Vous pouvez exclure de l'enregistrement d'événements la visibilité supplémentaire sur les objets supprimés. Pour plus d'informations, consultez les AWS CLI exemples de filtrage des événements de données dans le Guide de AWS CloudTrail l'utilisateur.

Pour configurer un journal de suivi afin de consigner les événements de données pour un compartiment S3, vous pouvez utiliser la console AWS CloudTrail ou la console Amazon S3. Si vous configurez un suivi pour consigner les événements de données pour tous les compartiments Amazon S3 de votre choix Compte AWS, il est plus facile d'utiliser la CloudTrail console. Pour plus d'informations sur l'utilisation de la CloudTrail console pour configurer un journal des événements liés aux données S3, consultez la section Événements liés aux données dans le guide de AWS CloudTrail l'utilisateur.

Important

Des frais supplémentaires sont facturés pour les événements de données. Pour en savoir plus, consultez Tarification de AWS CloudTrail.

La procédure suivante explique comment utiliser la console Amazon S3 pour configurer un journal afin de CloudTrail consigner les événements de données d'un compartiment S3.

Pour activer la journalisation des événements de CloudTrail données pour les objets d'un compartiment S3 à usage général ou d'un compartiment d'annuaire S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le nom du compartiment.
3. Choisissez Propriétés.
4. Sous Événements AWS CloudTrail liés aux données, sélectionnez Configurer dans CloudTrail.

   Vous pouvez créer une nouvelle CloudTrail trace ou réutiliser une trace existante et configurer les événements de données Amazon S3 pour qu'ils soient enregistrés dans votre trace. Pour plus d'informations sur la création de pistes dans la CloudTrail console, consultez la section Création et mise à jour d'une piste avec la console dans le guide de AWS CloudTrail l'utilisateur. Pour plus d'informations sur la configuration de la journalisation des événements de données

Amazon S3 dans la CloudTrail console, consultez la section Journalisation des événements de données pour les objets Amazon S3 dans le guide de AWS CloudTrail l'utilisateur.

> **Note**
>
> Si vous utilisez la CloudTrail console ou la console Amazon S3 pour configurer un journal afin de consigner les événements de données d'un compartiment S3, la console Amazon S3 indique que la journalisation au niveau de l'objet est activée pour le compartiment.

Pour désactiver la journalisation des événements de CloudTrail données pour les objets d'un compartiment S3

1. Connectez-vous à la CloudTrail console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudtrail/.
2. Dans le panneau de navigation de gauche, choisissez Journaux de suivi.
3. Choisissez le nom du journal de suivi que vous avez créé pour journaliser les événements de votre compartiment.
4. Sur la page de détails de votre journal de suivi, choisissez Arrêter la journalisation dans le coin supérieur droit.
5. Dans la boîte de dialogue qui s'affiche, cliquez sur Arrêter la journalisation.

Pour plus d'informations sur l'activation de la journalisation au niveau des objets lorsque vous créez un compartiment S3, consultez Création d'un bucket à usage général.

Pour plus d'informations sur la CloudTrail journalisation à l'aide de compartiments S3, consultez les rubriques suivantes :

- Afficher les propriétés d'un bucket S3 à usage général
- Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail
- Utilisation des fichiers CloudTrail journaux dans le guide de AWS CloudTrail l'utilisateur

Identification des demandes Amazon S3 à l'aide de CloudTrail

Dans Amazon S3, vous pouvez identifier les demandes à l'aide d'un journal d' AWS CloudTrail événements. AWS CloudTrail est la méthode préférée pour identifier les demandes Amazon S3,

mais si vous utilisez les journaux d'accès aux serveurs Amazon S3, consultezthe section called "Identification des demandes S3".

Rubriques

- Identification des demandes adressées à Amazon S3 dans un CloudTrail journal
- Identification des demandes Amazon S3 Signature version 2 à l'aide de CloudTrail
- Identification de l'accès aux objets S3 en utilisant CloudTrail

Identification des demandes adressées à Amazon S3 dans un CloudTrail journal

Une fois que vous avez configuré CloudTrail la transmission d'événements vers un compartiment, vous devriez commencer à voir des objets se diriger vers votre compartiment de destination sur la console Amazon S3. Ils se présentent dans le format suivant :

```
s3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/Region/yyyy/mm/dd
```

Les événements enregistrés par CloudTrail sont stockés sous forme d'objets gzipped JSON compressés dans votre compartiment S3. Pour rechercher efficacement les demandes, vous devez utiliser un service tel qu'Amazon Athena pour indexer et interroger les CloudTrail journaux.

Pour plus d'informations sur Athena CloudTrail et Athena, consultez la section Création de la table pour les AWS CloudTrail journaux dans Athena à l'aide de la projection de partitions dans le guide de l'utilisateur d'Amazon Athena.

Identification des demandes Amazon S3 Signature version 2 à l'aide de CloudTrail

Vous pouvez utiliser un journal d' CloudTrail événements pour identifier la version de signature d'API utilisée pour signer une demande dans Amazon S3. Cette fonctionnalité est importante étant donné que la prise en charge de Signature Version 2 va être désactivée (obsolète). Après cela, Amazon S3 n'acceptera plus les demandes utilisant Signature Version 2, et toutes les demandes devront utiliser le processus de signature Signature Version 4.

Nous vous recommandons vivement de l'utiliser CloudTrail pour déterminer si l'un de vos flux de travail utilise la signature Signature version 2. Pour y remédier, mettez à niveau vos bibliothèques et votre code afin qu'ils utilisent plutôt Signature Version 4 afin d'éviter tout impact sur votre entreprise.

Pour plus d'informations, consultez Annonce : AWS CloudTrail pour Amazon S3 ajoute de nouveaux champs pour un audit de sécurité amélioré dans AWS re:Post.

> **Note**
>
> CloudTrail les événements pour Amazon S3 incluent la version de signature dans les détails de la demande sous le nom de clé « »`additionalEventData`. Pour trouver la version de signature des demandes effectuées pour des objets dans Amazon S3`GET`, tels que,`PUT`, et des `DELETE` demandes, vous devez activer CloudTrail les événements de données. (Cette fonction est désactivée par défaut).

AWS CloudTrail est la méthode préférée pour identifier les demandes de signature version 2. Si vous utilisez les journaux d'accès au serveur Amazon S3, consultez Identification des demandes Signature Version 2 à l'aide des journaux d'accès Amazon S3.

Rubriques

- Exemples de requête Athena pour l'identification de demandes Amazon S3 Signature Version 2
- Partitionnement des données Signature Version 2

Exemples de requête Athena pour l'identification de demandes Amazon S3 Signature Version 2

Example — sélectionnez tous les événements de la version 2 de la signature et imprimez uniquement **`EventTime`**, **`S3_Action`**, **`Request_Parameters`**, **`Region`**, **`SourceIP`**, et **`UserAgent`**

Dans la requête Athena suivante, remplacez *`s3_cloudtrail_events_db.cloudtrail_table`* par vos coordonnées Athena, et augmentez ou supprimez la limite selon les besoins.

```
SELECT EventTime, EventName as S3_Action, requestParameters as Request_Parameters,
 awsregion as AWS_Region, sourceipaddress as Source_IP, useragent as User_Agent
FROM s3_cloudtrail_events_db.cloudtrail_table
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
LIMIT 10;
```

Example – Sélectionner tous les demandeurs qui envoient du trafic Signature Version 2

```
SELECT useridentity.arn, Count(requestid) as RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table
```

```
WHERE eventsource='s3.amazonaws.com'
    and json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
Group by useridentity.arn
```

Partitionnement des données Signature Version 2

Si vous devez interroger un large volume de données, vous pouvez réduire les coûts et l'exécution d'Athena en créant une table partitionnée.

Pour ce faire, créez une nouvelle table avec des partitions, comme suit.

```
CREATE EXTERNAL TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned(
     eventversion STRING,
     userIdentity STRUCT<
         type:STRING,
         principalid:STRING,
         arn:STRING,
         accountid:STRING,
         invokedby:STRING,
         accesskeyid:STRING,
         userName:STRING,
      sessioncontext:STRUCT<
                 attributes:STRUCT<
                 mfaauthenticated:STRING,
                 creationdate:STRING>,
                 sessionIssuer:STRUCT<
                 type:STRING,
                 principalId:STRING,
                 arn:STRING,
                 accountId:STRING,
                 userName:STRING>
             >
          >,
     eventTime STRING,
     eventSource STRING,
     eventName STRING,
     awsRegion STRING,
     sourceIpAddress STRING,
     userAgent STRING,
     errorCode STRING,
     errorMessage STRING,
```

```
        requestParameters STRING,
        responseElements STRING,
        additionalEventData STRING,
        requestId STRING,
        eventId STRING,
        resources ARRAY<STRUCT<ARN:STRING,accountId: STRING,type:STRING>>,
        eventType STRING,
        apiVersion STRING,
        readOnly STRING,
        recipientAccountId STRING,
        serviceEventDetails STRING,
        sharedEventID STRING,
        vpcEndpointId STRING
    )
    PARTITIONED BY (region string, year string, month string, day string)
    ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
    STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
    OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
    LOCATION 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/';
```

Ensuite, créez les partitions individuellement. Vous ne pouvez pas obtenir des résultats à partir de dates que vous n'avez pas créées.

```
ALTER TABLE s3_cloudtrail_events_db.cloudtrail_table_partitioned ADD
    PARTITION (region= 'us-east-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-east-1/2019/02/19/'
    PARTITION (region= 'us-west-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-1/2019/02/19/'
    PARTITION (region= 'us-west-2', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/us-west-2/2019/02/19/'
    PARTITION (region= 'ap-southeast-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-1/2019/02/19/'
    PARTITION (region= 'ap-southeast-2', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-southeast-2/2019/02/19/'
    PARTITION (region= 'ap-northeast-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/ap-northeast-1/2019/02/19/'
    PARTITION (region= 'eu-west-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/eu-west-1/2019/02/19/'
    PARTITION (region= 'sa-east-1', year= '2019', month= '02', day= '19') LOCATION
 's3://amzn-s3-demo-bucket1/AWSLogs/111122223333/CloudTrail/sa-east-1/2019/02/19/';
```

Vous pouvez ensuite effectuer la demande en fonction de ces partitions. Vous n'avez pas besoin de charger le compartiment entier.

```
SELECT useridentity.arn,
Count(requestid) AS RequestCount
FROM s3_cloudtrail_events_db.cloudtrail_table_partitioned
WHERE eventsource='s3.amazonaws.com'
AND json_extract_scalar(additionalEventData, '$.SignatureVersion')='SigV2'
AND region='us-east-1'
AND year='2019'
AND month='02'
AND day='19'
Group by useridentity.arn
```

Identification de l'accès aux objets S3 en utilisant CloudTrail

Vous pouvez utiliser vos journaux d' AWS CloudTrail événements pour identifier les demandes d'accès aux objets Amazon S3 relatives à des événements de données tels que `GetObject`DeleteObject, et`PutObject`, et découvrir des informations supplémentaires sur ces demandes.

> **Note**
>
> Si vous enregistrez une activité liée aux données avec AWS CloudTrail, l'enregistrement d'un événement de `DeleteObjects` données Amazon S3 inclut à la fois l'`DeleteObjects`événement et un `DeleteObject` événement pour chaque objet supprimé dans le cadre de cette opération. Vous pouvez exclure de l'enregistrement d'événements la visibilité supplémentaire sur les objets supprimés. Pour plus d'informations, consultez les AWS CLI exemples de filtrage des événements de données dans le Guide de AWS CloudTrail l'utilisateur.

L'exemple suivant montre comment obtenir toutes les demandes PUT d'objets pour Amazon S3 à partir d'un journal d' AWS CloudTrail événements.

Rubriques

- Exemples de requêtes Athena pour identifier les demandes d'accès aux objets Amazon S3

Exemples de requêtes Athena pour identifier les demandes d'accès aux objets Amazon S3

Dans les exemples de requêtes Athena suivants, remplacez *s3_cloudtrail_events_db.cloudtrail_table* par vos coordonnées Athena et modifiez la plage de dates si nécessaire.

Example — sélectionnez tous les événements pour lesquels il existe des demandes d'accès à des objets **PUT**, et imprimez uniquement **EventTime**, **EventSource**, **SourceIP**, **UserAgent**, **BucketName**, **object** et **UserARN**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  eventName = 'PutObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — sélectionnez tous les événements pour lesquels il existe des demandes d'accès à des objets **GET**, et imprimez uniquement **EventTime**, **EventSource**, **SourceIP**, **UserAgent**, **BucketName**, **object** et **UserARN**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  json_extract_scalar(requestParameters, '$.key') as object,
  userIdentity.arn as userArn
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
```

```
  eventName = 'GetObject'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — sélectionnez tous les événements des demandeurs anonymes dans un compartiment pendant une certaine période et imprimez seulement **`EventTime`**, **`EventName`**, **`EventSource`**, **`SourceIP`**, **`UserAgent`**, **`BucketName`**, **`UserARN`** et **`AccountID`**

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
  userIdentity.arn as userArn,
  userIdentity.accountId
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  userIdentity.accountId = 'anonymous'
  AND eventTime BETWEEN '2019-07-05T00:00:00Z' and '2019-07-06T00:00:00Z'
```

Example — identifiez toutes les demandes qui ont nécessité un ACL pour l'autorisation.

L'exemple de requête Amazon Athena suivant montre comment identifier toutes les requêtes de vos compartiments S3 qui ont nécessité une liste de contrôle d'accès (ACL) pour l'autorisation. Si la requête a nécessité une ACL pour l'autorisation, la valeur `aclRequired` dans `additionalEventData` est `Yes`. Si la réponse ACLs est négative, elle n'`aclRequired`est pas présente. Vous pouvez utiliser ces informations pour migrer ces autorisations ACL vers les politiques de compartiment appropriées. Après avoir créé ces politiques de compartiment, vous pouvez les désactiver ACLs pour ces compartiments. Pour plus d'informations sur la désactivation ACLs, consultezConditions préalables à la désactivation ACLs.

```
SELECT
  eventTime,
  eventName,
  eventSource,
  sourceIpAddress,
  userAgent,
  userIdentity.arn as userArn,
  json_extract_scalar(requestParameters, '$.bucketName') as bucketName,
```

```
  json_extract_scalar(requestParameters, '$.key') as object,
  json_extract_scalar(additionalEventData, '$.aclRequired') as aclRequired
FROM
  s3_cloudtrail_events_db.cloudtrail_table
WHERE
  json_extract_scalar(additionalEventData, '$.aclRequired') = 'Yes'
  AND eventTime BETWEEN '2022-05-10T00:00:00Z' and '2022-08-10T00:00:00Z'
```

> **Note**
>
> - Ces exemples de requêtes sont également utiles pour surveiller la sécurité. Vous pouvez vérifier les résultats pour les appels `PutObject` ou `GetObject` depuis des adresses IP ou des demandeurs inattendus ou non autorisés et pour identifier les demandes anonymes adressées à vos compartiments.
> - Cette requête ne récupère d'informations qu'à partir du moment où l'enregistrement a été activé.

Si vous utilisez les journaux d'accès au serveur Amazon S3, consultez Identification des demandes d'accès aux objets à l'aide des journaux d'accès Amazon S3.

Enregistrement de demandes avec journalisation des accès au serveur

La journalisation des accès au serveur fournit des enregistrements détaillés pour les demandes soumises à un compartiment. Les journaux d'accès au serveur sont utiles pour de nombreuses applications. Par exemple, les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Ces informations peuvent également vous aider à en savoir plus sur votre clientèle et à comprendre votre facture Amazon S3.

> **Note**
>
> Les journaux d'accès au serveur n'enregistrent pas les informations concernant les erreurs de redirection en cas de région incorrecte pour les régions lancées après le 20 mars 2019. Les erreurs de redirection en cas de région incorrecte se produisent lorsqu'une demande pour un objet ou un compartiment est effectuée en dehors de la région où se trouve le compartiment.

Comment activer la livraison des journaux ?

Suivez ces quelques étapes pour activer la livraison des journaux. Pour plus d'informations, consultez Activation de la journalisation des accès au serveur Amazon S3.

1. Indiquez le nom du compartiment de destination (également appelé compartiment cible). Amazon S3 enregistrera dans ce compartiment les journaux d'accès en tant qu'objets. Les compartiments source et de destination doivent être dans la même Région AWS et appartenir au même compte. Le compartiment de destination ne doit pas avoir de configuration de période de rétention par défaut pour le verrouillage d'objet S3. Le paiement par le demandeur ne doit pas non plus être activé pour le compartiment de destination.

   Les journaux peuvent être fournis dans n'importe quel compartiment que vous possédez qui est situé dans la même Région que le compartiment source, y compris le compartiment source lui-même. Mais pour simplifier la gestion des journaux, nous vous recommandons d'enregistrer les journaux d'accès dans un autre compartiment.

   Lorsque votre compartiment source et votre compartiment de destination correspondent au même compartiment, des journaux supplémentaires sont créés pour les journaux qui sont écrits dans le compartiment, ce qui crée une boucle infinie de journaux. Nous ne recommandons pas de procéder ainsi, car cela peut entraîner une légère augmentation de votre facture de stockage. En outre, les journaux supplémentaires concernant les journaux peuvent rendre plus difficile la recherche du journal que vous recherchez.

   Si vous choisissez d'enregistrer les journaux d'accès dans le compartiment source, nous vous recommandons de spécifier un préfixe de destination (également appelé préfixe cible) pour toutes les clés d'objets journaux. Lorsque vous spécifiez un préfixe, tous les noms des objets journaux commencent par une chaîne commune, ce qui facilite l'identification des objets journaux.
2. (Facultatif) Affectez un préfixe de destination à toutes les clés d'objets journaux Amazon S3. Le préfixe de destination (également appelé préfixe cible) vous aide à localiser les objets journaux. Par exemple, si vous spécifiez la valeur de préfixe `logs/`, chaque objet journal créé par Amazon S3 commence par le préfixe `logs/` dans sa clé, par exemple :

   ```
   logs/2013-11-01-21-32-16-E568B2907131C0C0
   ```

   Si vous spécifiez la valeur de préfixe `logs`, l'objet journal apparaît comme suit :

```
logs2013-11-01-21-32-16-E568B2907131C0C0
```

Les préfixes sont également utiles pour distinguer les compartiments sources lorsque plusieurs compartiments sont journalisés dans le même compartiment de destination.

Ce préfixe peut également s'avérer utile lors de la suppression des journaux. Par exemple, vous pouvez définir une règle de configuration du cycle de vie pour qu'Amazon S3 supprime les objets dotés d'un préfixe spécifique. Pour plus d'informations, consultez Suppression des fichiers journaux Amazon S3.

3. (Facultatif) Définissez des autorisations pour que d'autres utilisateurs puissent accéder aux journaux générés. Par défaut, seul le propriétaire du compartiment possède un accès total aux objets des journaux. Si votre compartiment de destination utilise le paramètre imposé par le propriétaire du compartiment pour S3 Object Ownership afin de désactiver les listes de contrôle d'accès (ACLs), vous ne pouvez pas accorder d'autorisations dans les autorisations de destination (également appelées autorisations cibles) qui utilisent ACLs. Toutefois, vous pouvez mettre à jour votre politique de compartiment pour le compartiment de destination afin d'accorder l'accès à d'autres personnes. Pour plus d'informations, consultez Gestion des identités et des accès pour Amazon S3 et Autorisations de diffusion de journaux.
4. (Facultatif) Définissez un format de clé d'objet journal pour les fichiers journaux. Deux options s'offrent à vous pour le format de clé d'objet journal (également appelé format de clé d'objet cible) :

   - Non-date-based partitionnement — Il s'agit du format de clé de l'objet journal d'origine. Si vous choisissez ce format, le format de clé de fichier journal apparaît comme suit :

     ```
     [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
     ```

     Par exemple, si vous spécifiez `logs/` comme préfixe, vos objets journaux sont nommés comme suit :

     ```
     logs/2013-11-01-21-32-16-E568B2907131C0C0
     ```

   - Partitionnement basé sur la date : si vous choisissez un partitionnement basé sur la date, vous pouvez choisir l'heure de l'événement ou l'heure de livraison du fichier journal comme source de date utilisée dans le format de journal. Ce format facilite l'interrogation des journaux.

     Si vous choisissez un partitionnement basé sur la date, le format de clé de fichier journal apparaît comme suit :

```
[DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/
[DD]/[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

Par exemple, si vous spécifiez `logs/` comme préfixe cible, vos objets journaux sont nommés comme suit :

```
logs/123456789012/us-west-2/amzn-s3-demo-source-
bucket/2023/03/01/2023-03-01-21-32-16-E568B2907131C0C0
```

Pour la livraison de l'heure de livraison, l'heure indiquée dans les noms des fichiers journaux correspond à l'heure de livraison des fichiers journaux.

Pour la livraison de l'heure d'événement, l'année, le mois et le jour correspondent au jour où l'événement s'est produit, et l'heure, les minutes et les secondes sont définies sur `00` dans la clé. Les journaux livrés dans ces fichiers journaux se rapportent à un jour spécifique uniquement.

Si vous configurez vos journaux via AWS Command Line Interface (AWS CLI) ou l'API REST Amazon S3 AWS SDKs, utilisez-le `TargetObjectKeyFormat` pour spécifier le format de clé de l'objet du journal. Pour spécifier le non-date-based partitionnement, utilisez`SimplePrefix`. Pour spécifier un partitionnement basé sur la date, utilisez `PartitionedPrefix`. Si vous utilisez `PartitionedPrefix`, utilisez `PartitionDateSource` pour spécifier `EventTime` ou `DeliveryTime`.

Pour `SimplePrefix`, le format de clé de fichier journal apparaît comme suit :

```
[TargetPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

Pour `PartitionedPrefix` avec l'heure d'événement ou l'heure de livraison, le format de clé de fichier journal apparaît comme suit :

```
[TargetPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
```

Format de clé d'objet journal

Amazon S3 utilise les formats de clé d'objet suivants pour les objets journaux qu'il charge dans le compartiment de destination :

- Non-date-based partitionnement — Il s'agit du format de clé de l'objet journal d'origine. Si vous choisissez ce format, le format de clé de fichier journal apparaît comme suit :

  ```
  [DestinationPrefix][YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

- Partitionnement basé sur la date : si vous choisissez un partitionnement basé sur la date, vous pouvez choisir l'heure de l'événement ou l'heure de livraison du fichier journal comme source de date utilisée dans le format de journal. Ce format facilite l'interrogation des journaux.

  Si vous choisissez un partitionnement basé sur la date, le format de clé de fichier journal apparaît comme suit :

  ```
  [DestinationPrefix][SourceAccountId]/[SourceRegion]/[SourceBucket]/[YYYY]/[MM]/[DD]/
  [YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
  ```

Dans la clé d'objet journal, `YYYY`, `MM`, `DD`, `hh`, `mm` et `ss` correspondent (respectivement) à l'année, au mois, au jour, aux heures, aux minutes et aux secondes. Ces dates et heures sont exprimées en heure UTC (temps universel coordonné).

Un fichier journal distribué à un moment précis peut contenir des enregistrements écrits à tout moment avant ce moment. Il n'existe aucun moyen de savoir si tous les enregistrements d'un intervalle de temps donné ont été distribués.

Le composant `UniqueString` de la clé empêche le remplacement des fichiers. Il n'a aucune signification, et doit être ignoré par les logiciels de traitement des journaux.

Comment sont distribués les journaux ?

Amazon S3 collecte régulièrement les enregistrements des journaux d'accès, consolide ces enregistrements dans des fichiers journaux, puis charge les fichiers journaux dans le compartiment de destination comme objets journaux. Si vous activez la journalisation sur plusieurs compartiments sources qui identifient le même compartiment de destination, ce dernier dispose de journaux d'accès pour tous ces compartiments sources. Cependant, chaque objet journal contient des enregistrements de journal d'accès pour un compartiment source spécifique.

Amazon S3 utilise un compte de livraison de journaux spécial pour écrire des journaux d'accès au serveur. Ces journaux sont sujets aux restrictions habituelles de contrôle d'accès en écriture. Nous vous recommandons de mettre à jour la politique de compartiment sur le compartiment de destination pour accorder l'accès au principal du service de journalisation (`logging.s3.amazonaws.com`) pour la livraison des journaux des accès. Vous pouvez également accorder l'accès pour la livraison des journaux des d'accès au groupe de livraison des journaux S3 via votre liste de contrôle d'accès (ACL) de compartiment. Toutefois, il n'est pas recommandé d'accorder l'accès au groupe de livraison des journaux S3 en utilisant votre liste ACL de compartiment.

Lorsque vous activez la journalisation des accès au serveur et que vous accordez l'accès à la livraison des journaux des accès via votre politique de compartiment de destination, vous devez mettre à jour la politique pour autoriser l'accès `s3:PutObject` pour le principal du service de journalisation. Si vous utilisez la console Amazon S3 pour activer la journalisation des accès au serveur, la console met automatiquement à jour la politique de compartiment de destination, afin d'accorder ces autorisations au principal du service de journalisation. Pour plus d'informations sur l'accord d'autorisations pour la livraison de journaux d'accès au serveur, consultez Autorisations de diffusion de journaux.

> **Note**
>
> S3 ne prend pas en charge la livraison de CloudTrail journaux ou de journaux d'accès au serveur au demandeur ou au propriétaire du compartiment pour les demandes de point de terminaison VPC lorsque la politique de point de terminaison du VPC les refuse ou pour les demandes qui échouent avant que la politique VPC ne soit évaluée.

Paramètre bucket owner enforced (propriétaire du compartiment imposé) pour S3 Object Ownership (Propriété de l'objet S3)

Si le compartiment de destination utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets, ACLs ils sont désactivés et n'affectent plus les autorisations. Vous devez mettre à jour la politique de compartiment sur le compartiment de destination pour accorder l'accès au principal du service de journalisation. Pour en savoir plus sur la propriété des objets, consultez Octroi de l'accès au groupe de livraison des journaux S3 pour la journalisation des accès au serveur.

Livraison des journaux du serveur dans la mesure du possible

Les enregistrements des journaux d'accès au serveur sont fournis dans la mesure du possible. La plupart des demandes pour un compartiment correctement configuré pour l'enregistrement se

traduisent par un enregistrement de journal distribué. La plupart des enregistrements de journal sont fournis quelques heures après leur enregistrement, mais ils peuvent être livrés plus fréquemment.

L'exhaustivité et la disponibilité de la journalisation du serveur ne sont pas garanties. Il se peut que l'enregistrement du journal pour une demande particulière soit fourni bien après le traitement de la demande, ou ne soit fourni du tout. Il est même possible que vous voyiez une duplication d'un enregistrement de journal. Le but des journaux du serveur est de vous donner une idée de la nature du trafic dans le compartiment. Bien qu'il soit rare de perdre des enregistrements de journaux ou de constater une duplication d'enregistrements de journaux, sachez que la journalisation du serveur n'a pas pour but de comptabiliser toutes les demandes.

En raison de la nature de la journalisation du serveur, visant un effort maximal, vos rapports d'utilisation peuvent inclure une ou plusieurs demandes qui n'apparaissent pas dans un journal de serveur livré. Ces rapports d'utilisation se trouvent sous Rapports d'utilisation et de coût dans la console AWS Billing and Cost Management .

Les changements de statut de la journalisation des compartiments prennent effet au fil du temps

Les modifications du statut de l'état de journalisation d'un compartiment prennent du temps avant d'affecter réellement la distribution des fichiers journaux. Par exemple, si vous activez la journalisation pour un compartiment, certaines demandes faites dans l'heure qui suit peuvent être journalisées, alors que d'autres ne le sont pas. Supposons que vous changiez le compartiment de destination de la journalisation du compartiment A au compartiment B. L'heure suivante, certains journaux peuvent continuer à être livrés dans le compartiment A, tandis que d'autres peuvent être livrés dans le nouveau compartiment de destination B. Dans tous les cas, les nouveaux paramètres finissent par prendre effet sans aucune autre action de votre part.

Pour plus d'informations sur la journalisation et les fichiers journaux, consultez les sections suivantes :

Rubriques

- Activation de la journalisation des accès au serveur Amazon S3
- Format des journaux d'accès au serveur Amazon S3
- Suppression des fichiers journaux Amazon S3
- Utilisation des journaux d'accès au serveur Amazon S3 pour identifier des demandes
- Résolution des problèmes de journalisation des accès au serveur

Activation de la journalisation des accès au serveur Amazon S3

La journalisation des accès au serveur fournit des enregistrements détaillés des demandes soumises à un compartiment Amazon S3. Les journaux d'accès au serveur sont utiles pour de nombreuses applications. Par exemple, les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Ces informations peuvent également vous aider à en savoir plus sur votre clientèle et à comprendre votre facture Amazon S3.

Par défaut, Amazon S3 ne collecte pas les journaux d'accès au serveur. Lorsque vous activez la journalisation, Amazon S3 fournit les journaux d'accès pour un compartiment source dans un compartiment de destination (également appelé compartiment cible) de votre choix. Le compartiment de destination doit se trouver dans le même Région AWS compartiment Compte AWS que le compartiment source.

Un enregistrement de journal d'accès contient des détails relatifs aux demandes soumises à un compartiment. Ces informations peuvent comprendre le type de demande, les ressources spécifiées dans la demande, ainsi que l'heure et la date du traitement de la demande. Pour plus d'informations sur les principes de base de la journalisation, consultez Enregistrement de demandes avec journalisation des accès au serveur.

Important

- L'activation de la journalisation des accès au serveur sur un compartiment Amazon S3 n'entraîne aucuns frais supplémentaires. Toutefois, les fichiers journaux qui vous sont fournis par le système augmentent les coûts de stockage habituels. Notez que vous pouvez supprimer les fichiers journaux à tout moment. Nous n'évaluons pas les frais de transfert de données pour la livraison des fichiers journaux, mais nous facturons les frais standard de transfert de données pour l'accès aux fichiers journaux.
- La journalisation des accès au serveur de votre compartiment de destination ne doit pas être activée. Les journaux peuvent être fournis dans n'importe quel compartiment que vous possédez qui est situé dans la même Région que le compartiment source, y compris le compartiment source lui-même. Toutefois, la livraison de journaux vers le compartiment source entraîne une boucle infinie de journaux et n'est pas recommandée. Pour simplifier la gestion des journaux, nous vous recommandons d'enregistrer les journaux d'accès dans un autre compartiment. Pour plus d'informations, consultez Comment activer la livraison des journaux ?.

- Les compartiments S3 sur lesquels le verrouillage d'objet S3 est activé ne peuvent pas être utilisés comme compartiments de destination pour les journaux d'accès au serveur. Votre compartiment de destination ne doit pas avoir de configuration de période de rétention par défaut.
- Le paiement par le demandeur ne doit pas être activé pour le compartiment de destination.
- Vous pouvez utiliser le chiffrement de compartiment par défaut sur le compartiment de destination seulement si vous utilisez le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), qui utilise la norme Advanced Encryption Standard à 256 bits (AES-256). Le chiffrement côté serveur par défaut avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) n'est pas pris en charge.

Vous pouvez activer ou désactiver la journalisation des accès au serveur à l'aide de la console Amazon S3, de l'API Amazon S3, du AWS Command Line Interface (AWS CLI) ou AWS SDKs.

Autorisations de diffusion de journaux

Amazon S3 utilise un compte de livraison de journaux spécial pour écrire des journaux d'accès au serveur. Ces journaux sont sujets aux restrictions habituelles de contrôle d'accès en écriture. Pour la livraison des journaux des accès, vous devez accorder au principal du service de journalisation (`logging.s3.amazonaws.com`) l'accès à votre compartiment de destination.

Pour accorder des autorisations à Amazon S3 pour la livraison de logs, vous pouvez utiliser une politique de compartiment ou des listes de contrôle d'accès aux compartiments (ACLs), en fonction des paramètres de propriété des objets S3 de votre compartiment de destination. Cependant, nous vous recommandons d'utiliser une politique de compartiment à la place de ACLs.

Paramètre bucket owner enforced (propriétaire du compartiment imposé) pour S3 Object Ownership (Propriété de l'objet S3)

Si le compartiment de destination utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets, ACLs ils sont désactivés et n'affectent plus les autorisations. Dans ce cas, vous devez mettre à jour la politique de compartiment pour le compartiment de destination afin d'accorder l'accès au principal du service de journalisation. Vous ne pouvez pas mettre à jour la liste ACL de votre compartiment pour accorder l'accès au groupe de mise à disposition des journaux S3. Vous ne pouvez pas non plus inclure des octrois de destination (également appelés octrois cibles) dans votre configuration PutBucketLogging.

Pour plus d'informations sur la migration d'un bucket existant ACLs pour la livraison des journaux d'accès vers une politique de bucket, consultezOctroi de l'accès au groupe de livraison des journaux S3 pour la journalisation des accès au serveur. Pour en savoir plus sur la propriété des objets, consultez Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment. Lorsque vous créez de nouveaux compartiments, ACLs ils sont désactivés par défaut.

Octroi d'accès à l'aide d'une politique de compartiment

Pour accorder l'accès en utilisant la politique de compartiment sur le compartiment de destination, mettez à jour la politique de compartiment afin d'accorder l'autorisation `s3:PutObject` au principal du service de journalisation. Si vous utilisez la console Amazon S3 pour activer la journalisation des accès au serveur, la console met automatiquement à jour la politique de compartiment sur le compartiment de destination, afin d'accorder cette autorisation au principal du service de journalisation. Si vous activez la journalisation des accès au serveur par programmation, vous devez mettre à jour manuellement la politique de compartiment pour le compartiment de destination afin d'accorder l'accès au principal du service de journalisation.

Pour un exemple de politique de compartiment qui accorde l'accès au principal du service de journalisation, consultez the section called "Octroi d'autorisations au principal du service de journalisation à l'aide d'une politique de compartiment".

Octroi d'accès à l'aide d'un bucket ACLs

Vous pouvez également utiliser un bucket ACLs pour accorder l'accès à la livraison du journal d'accès. Vous ajoutez une entrée d'accord à la liste ACL du compartiment qui accorde les autorisations `WRITE` et `READ_ACP` sur le groupe de mise à disposition des journaux S3. Toutefois, il n' ACLs est pas recommandé d'accorder l'accès au groupe de distribution de journaux S3 à l'aide d'un bucket. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment. Pour plus d'informations sur la migration d'un bucket existant ACLs pour la livraison des journaux d'accès vers une politique de bucket, consultezOctroi de l'accès au groupe de livraison des journaux S3 pour la journalisation des accès au serveur. Pour obtenir un exemple de liste ACL qui accorde l'accès au principal du service de journalisation, consultez the section called "Octroi d'autorisations au groupe de livraison des journaux à l'aide d'une liste ACL de compartiment".

Octroi d'autorisations au principal du service de journalisation à l'aide d'une politique de compartiment

Cet exemple de politique de compartiment accorde l'autorisation `s3:PutObject` au principal du service de journalisation (`logging.s3.amazonaws.com`). Pour utiliser cette politique de

compartiment, remplacez *user input placeholders* par vos propres informations. Dans la politique suivante, *amzn-s3-demo-destination-bucket* il s'agit du compartiment de destination dans lequel les journaux d'accès au serveur seront fournis et *amzn-s3-demo-source-bucket* du compartiment source. *EXAMPLE-LOGGING-PREFIX*est le préfixe de destination facultatif (également appelé préfixe cible) que vous souhaitez utiliser pour vos objets de journal. *SOURCE-ACCOUNT-ID*est celui Compte AWS qui possède le compartiment source.

> **Note**
>
> Si votre politique de compartiment contient des instructions `Deny`, veillez à ce qu'elles n'empêchent pas Amazon S3 de livrer les journaux d'accès.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3ServerAccessLogsPolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "logging.s3.amazonaws.com"
            },
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket/EXAMPLE-
LOGGING-PREFIX*",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

Octroi d'autorisations au groupe de livraison des journaux à l'aide d'une liste ACL de compartiment

> **Note**
>
> Pour des raisons de sécurité, Amazon S3 désactive les listes de contrôle d'accès (ACLs) par défaut dans tous les nouveaux compartiments. Pour plus d'informations sur les autorisations ACL dans la console Amazon S3, consultez Configuration ACLs.

Nous ne recommandons pas cette approche, mais vous pouvez accorder des autorisations au groupe de livraison des journaux en utilisant une liste ACL de compartiment. Toutefois, si le compartiment de destination utilise le paramètre imposé par le propriétaire du compartiment pour la propriété de l'objet, vous ne pouvez pas définir de compartiment ou d'objet ACLs. Vous ne pouvez pas non plus inclure des octrois de destination (également appelés octrois cibles) dans votre configuration PutBucketLogging. À la place, vous devez utiliser une politique de compartiment pour accorder l'accès au principal du service de journalisation (`logging.s3.amazonaws.com`). Pour plus d'informations, consultez Autorisations de diffusion de journaux.

Dans la liste ACL de compartiment, le groupe de livraison des journaux est représenté par l'URL suivante :

```
http://acs.amazonaws.com/groups/s3/LogDelivery
```

Pour accorder des autorisations `WRITE` et `READ_ACP` (lecture de liste ACL), ajoutez les octrois suivants à la liste ACL du compartiment de destination :

```
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>WRITE</Permission>
</Grant>
<Grant>
    <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"  xsi:type="Group">
        <URI>http://acs.amazonaws.com/groups/s3/LogDelivery</URI>
    </Grantee>
    <Permission>READ_ACP</Permission>
</Grant>
```

Pour obtenir des exemples d'ajout d'attributions ACL par programmation, consultez Configuration ACLs.

> **Important**
>
> Lorsque vous activez la journalisation de l'accès au serveur Amazon S3 AWS CloudFormation à l'aide d'un compartiment et que vous l'utilisez ACLs pour accorder l'accès au groupe de mise à disposition des journaux S3, vous devez également ajouter « » `AccessControl": "LogDeliveryWrite"` à votre CloudFormation modèle. Cela est important car vous ne pouvez accorder ces autorisations qu'en créant une ACL pour le bucket, mais vous ne pouvez pas créer de version personnalisée ACLs pour les buckets. CloudFormation Vous ne pouvez utiliser que des conserves ACLs avec CloudFormation.

Pour activer la journalisation des accès au serveur

Pour activer la journalisation des accès au serveur à l'aide de la console Amazon S3, de l'API REST Amazon S3 AWS SDKs AWS CLI, et suivez les procédures suivantes.

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer la journalisation des accès au serveur.
4. Choisissez Propriétés.
5. Dans la section Server access logging (Journalisation des accès au serveur) choisissez Edit (Modifier).
6. Sous Consignation des accès au serveur, choisissez Activer.
7. Sous Compartiment de destination, spécifiez un compartiment et un préfixe facultatif. Si vous spécifiez un préfixe, nous vous recommandons d'inclure une barre oblique (/) après le préfixe pour faciliter la recherche des journaux.

> **Note**
>
> La spécification d'un préfixe avec une barre oblique (/) simplifie la localisation des objets journaux. Par exemple, si vous spécifiez la valeur de préfixe `logs/`, chaque objet journal créé par Amazon S3 commence par le préfixe `logs/` dans sa clé, comme suit :
>
> ```
> logs/2013-11-01-21-32-16-E568B2907131C0C0
> ```
>
> Si vous spécifiez la valeur de préfixe `logs`, l'objet journal apparaît comme suit :
>
> ```
> logs2013-11-01-21-32-16-E568B2907131C0C0
> ```

8. Sous Format de clé d'objet journal, effectuez l'une des opérations suivantes :

   - Pour choisir le non-date-based partitionnement, choisissez [DestinationPrefix] [YYYY] - [MM] - [DD] - [hh] - [mm] - [ss] - []. UniqueString
   - Pour choisir le partitionnement basé sur la date, choisissez [DestinationPrefix] [SourceAccountId]/[SourceRegion]/[YYYYSourceBucket]/[MM]/[DD]/[YYYY] - [MM] - [DD] - [hh] - [mm] - [ss] - [UniqueString], puis choisissez l'heure de l'événement S3 ou l'heure de livraison du fichier journal.

9. Sélectionnez Enregistrer les modifications.

   Lorsque vous activez la journalisation des accès au serveur sur un compartiment, la console active la journalisation sur le compartiment source et met à jour la politique de compartiment pour le compartiment de destination afin d'accorder l'autorisation `s3:PutObject` au principal du service de journalisation (`logging.s3.amazonaws.com`). Pour plus d'informations sur cette politique de compartiment, consultez Octroi d'autorisations au principal du service de journalisation à l'aide d'une politique de compartiment.

   Vous pouvez afficher les journaux dans le compartiment de destination. Une fois que vous avez activé la journalisation des accès au serveur, cela peut prendre quelques heures avant que les journaux sont livrés dans le compartiment cible. Pour plus d'informations sur la façon et le moment de livraison des journaux, consultez Comment sont distribués les journaux ?.

Pour plus d'informations, consultez Afficher les propriétés d'un bucket S3 à usage général.

Utilisation de l'API REST

Pour activer la journalisation, vous envoyez une demande PutBucketLogging pour ajouter la configuration de journalisation sur le compartiment source. La demande spécifie le compartiment de destination (également appelé compartiment cible) et, si vous le souhaitez, le préfixe à utiliser avec toutes les clés d'objets journaux.

L'exemple suivant identifie *amzn-s3-demo-destination-bucket* comme compartiment de destination et *logs/* comme préfixe.

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
  </LoggingEnabled>
</BucketLoggingStatus>
```

L'exemple suivant identifie *amzn-s3-demo-destination-bucket* comme compartiment de destination, *logs/* comme préfixe et `EventTime` comme format de clé d'objet journal.

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
  <LoggingEnabled>
    <TargetBucket>amzn-s3-demo-destination-bucket</TargetBucket>
    <TargetPrefix>logs/</TargetPrefix>
    <TargetObjectKeyFormat>
      <PartitionedPrefix>
         <PartitionDateSource>EventTime</PartitionDateSource>
      </PartitionedPrefix>
  </TargetObjectKeyFormat>
  </LoggingEnabled>
</BucketLoggingStatus>
```

Les objets des journaux sont écrits et détenus par le compte de livraison des journaux S3, et le propriétaire du compartiment possède les autorisations complètes sur ces objets. Vous pouvez éventuellement utiliser des octrois de destination (également appelés octrois cibles) pour accorder des autorisations aux autres utilisateurs, afin qu'ils puissent accéder aux journaux. Pour de plus amples informations, veuillez consulter PutBucketLogging.

> **Note**
>
> Si le compartiment de destination utilise le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets, vous ne pouvez pas utiliser les octrois de destination pour accorder des autorisations à d'autres utilisateurs. Pour accorder des autorisations à d'autres, vous pouvez mettre à jour la politique de compartiment sur le compartiment de destination. Pour plus d'informations, consultez Autorisations de diffusion de journaux.

Pour récupérer la configuration de journalisation sur un compartiment, utilisez l'opération d'API GetBucketLogging.

Pour supprimer la configuration de la journalisation, vous envoyez une demande `PutBucketLogging` avec un paramètre `BucketLoggingStatus` vide :

```
<BucketLoggingStatus xmlns="http://doc.s3.amazonaws.com/2006-03-01">
</BucketLoggingStatus>
```

Pour activer la connexion à un compartiment, vous pouvez utiliser l'API Amazon S3 ou les bibliothèques d'encapsulation du AWS SDK.

À l'aide du AWS SDKs

Les exemples suivants activent la journalisation sur un compartiment. Vous devez créer deux compartiments : un compartiment source et un compartiment de destination (cible). Les exemples commencent par mettre à jour la liste ACL de compartiment sur le compartiment de destination. Ils accordent alors au groupe de livraison des journaux les autorisations nécessaires pour écrire des journaux dans le compartiment de destination, puis activent la journalisation sur le compartiment source.

Ces exemples ne fonctionnent pas sur les compartiments de destination qui utilisent le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets.

Si le compartiment de destination (cible) utilise le paramètre imposé par le propriétaire du compartiment pour la propriété de l'objet, vous ne pouvez pas définir de compartiment ou d'objet ACLs. Vous ne pouvez pas non plus inclure d'autorisations de destination (cible) dans votre PutBucketLoggingconfiguration. Vous devez utiliser une politique de compartiment pour accorder l'accès au principal du service de journalisation (`logging.s3.amazonaws.com`). Pour de plus amples informations, veuillez consulter Autorisations de diffusion de journaux.

.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 de code AWS.

```
using System;
using System.IO;
using System.Threading.Tasks;
using Amazon.S3;
using Amazon.S3.Model;
using Microsoft.Extensions.Configuration;

/// <summary>
/// This example shows how to enable logging on an Amazon Simple Storage
/// Service (Amazon S3) bucket. You need to have two Amazon S3 buckets for
/// this example. The first is the bucket for which you wish to enable
/// logging, and the second is the location where you want to store the
/// logs.
/// </summary>
public class ServerAccessLogging
{
    private static IConfiguration _configuration = null!;

    public static async Task Main()
    {
        LoadConfig();

        string bucketName = _configuration["BucketName"];
        string logBucketName = _configuration["LogBucketName"];
        string logObjectKeyPrefix = _configuration["LogObjectKeyPrefix"];
        string accountId = _configuration["AccountId"];

        // If the AWS Region defined for your default user is different
        // from the Region where your Amazon S3 bucket is located,
        // pass the Region name to the Amazon S3 client object's constructor.
        // For example: RegionEndpoint.USWest2 or RegionEndpoint.USEast2.
        IAmazonS3 client = new AmazonS3Client();
```

```
            try
            {
                // Update bucket policy for target bucket to allow delivery of
logs to it.
                await SetBucketPolicyToAllowLogDelivery(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix,
                    accountId);

                // Enable logging on the source bucket.
                await EnableLoggingAsync(
                    client,
                    bucketName,
                    logBucketName,
                    logObjectKeyPrefix);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine($"Error: {e.Message}");
            }
        }

        /// <summary>
        /// This method grants appropriate permissions for logging to the
        /// Amazon S3 bucket where the logs will be stored.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
used
        /// to apply the bucket policy.</param>
        /// <param name="sourceBucketName">The name of the source bucket.</param>
        /// <param name="logBucketName">The name of the bucket where logging
        /// information will be stored.</param>
        /// <param name="logPrefix">The logging prefix where the logs should be
delivered.</param>
        /// <param name="accountId">The account id of the account where the
source bucket exists.</param>
        /// <returns>Async task.</returns>
        public static async Task SetBucketPolicyToAllowLogDelivery(
            IAmazonS3 client,
            string sourceBucketName,
            string logBucketName,
```

```
            string logPrefix,
            string accountId)
        {
            var resourceArn = @"""arn:aws:s3:::" + logBucketName + "/" +
logPrefix + @"*""";

            var newPolicy = @"{
                                ""Statement"":[{
                                ""Sid"": ""S3ServerAccessLogsPolicy"",
                                ""Effect"": ""Allow"",
                                ""Principal"": { ""Service"":
""logging.s3.amazonaws.com"" },
                                ""Action"": [""s3:PutObject""],
                                ""Resource"": [" + resourceArn + @"],
                                ""Condition"": {
                                ""ArnLike"": { ""aws:SourceArn"":
""arn:aws:s3:::" + sourceBucketName + @""" },
                                ""StringEquals"": { ""aws:SourceAccount"": """ +
accountId + @""" }
                                        }
                                    }]
                                }";
            Console.WriteLine($"The policy to apply to bucket {logBucketName} to
enable logging:");
            Console.WriteLine(newPolicy);

            PutBucketPolicyRequest putRequest = new PutBucketPolicyRequest
            {
                BucketName = logBucketName,
                Policy = newPolicy,
            };
            await client.PutBucketPolicyAsync(putRequest);
            Console.WriteLine("Policy applied.");
        }

        /// <summary>
        /// This method enables logging for an Amazon S3 bucket. Logs will be
stored
        /// in the bucket you selected for logging. Selected prefix
        /// will be prepended to each log object.
        /// </summary>
        /// <param name="client">The initialized Amazon S3 client which will be
used
```

```
        /// to configure and apply logging to the selected Amazon S3 bucket.</
param>
        /// <param name="bucketName">The name of the Amazon S3 bucket for which
 you
        /// wish to enable logging.</param>
        /// <param name="logBucketName">The name of the Amazon S3 bucket where
 logging
        /// information will be stored.</param>
        /// <param name="logObjectKeyPrefix">The prefix to prepend to each
        /// object key.</param>
        /// <returns>Async task.</returns>
        public static async Task EnableLoggingAsync(
            IAmazonS3 client,
            string bucketName,
            string logBucketName,
            string logObjectKeyPrefix)
        {
            Console.WriteLine($"Enabling logging for bucket {bucketName}.");
            var loggingConfig = new S3BucketLoggingConfig
            {
                TargetBucketName = logBucketName,
                TargetPrefix = logObjectKeyPrefix,
            };

            var putBucketLoggingRequest = new PutBucketLoggingRequest
            {
                BucketName = bucketName,
                LoggingConfig = loggingConfig,
            };
            await client.PutBucketLoggingAsync(putBucketLoggingRequest);
            Console.WriteLine($"Logging enabled.");
        }

        /// <summary>
        /// Loads configuration from settings files.
        /// </summary>
        public static void LoadConfig()
        {
            _configuration = new ConfigurationBuilder()
                .SetBasePath(Directory.GetCurrentDirectory())
                .AddJsonFile("settings.json") // Load settings from .json file.
                .AddJsonFile("settings.local.json", true) // Optionally, load
 local settings.
                .Build();
```

```
        }
    }
```

- Pour plus de détails sur l'API, reportez-vous PutBucketLoggingà la section Référence des AWS SDK pour .NET API.

Java

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3.S3Client;
import software.amazon.awssdk.services.s3.model.BucketLoggingStatus;
import software.amazon.awssdk.services.s3.model.LoggingEnabled;
import software.amazon.awssdk.services.s3.model.PartitionedPrefix;
import software.amazon.awssdk.services.s3.model.PutBucketLoggingRequest;
import software.amazon.awssdk.services.s3.model.TargetObjectKeyFormat;

// Class to set a bucket policy on a target S3 bucket and enable server access
 logging on a source S3 bucket.
public class ServerAccessLogging {
    private static S3Client s3Client;

    public static void main(String[] args) {
        String sourceBucketName = "SOURCE-BUCKET";
        String targetBucketName = "TARGET-BUCKET";
        String sourceAccountId = "123456789012";
        String targetPrefix = "logs/";

        // Create S3 Client.
        s3Client = S3Client.builder().
                region(Region.US_EAST_2)
                .build();

        // Set a bucket policy on the target S3 bucket to enable server access
 logging by granting the
        // logging.s3.amazonaws.com principal permission to use the PutObject
 operation.
        ServerAccessLogging serverAccessLogging = new ServerAccessLogging();
        serverAccessLogging.setTargetBucketPolicy(sourceAccountId, sourceBucketName,
 targetBucketName);
```

```
        // Enable server access logging on the source S3 bucket.
        serverAccessLogging.enableServerAccessLogging(sourceBucketName,
 targetBucketName,
                targetPrefix);

    }

    // Function to set a bucket policy on the target S3 bucket to enable server
 access logging by granting the
    // logging.s3.amazonaws.com principal permission to use the PutObject operation.
    public void setTargetBucketPolicy(String sourceAccountId, String
 sourceBucketName, String targetBucketName) {
        String policy = "{\n" +
                "    \"Version\": \"2012-10-17\",\n" +
                "    \"Statement\": [\n" +
                "        {\n" +
                "            \"Sid\": \"S3ServerAccessLogsPolicy\",\n" +
                "            \"Effect\": \"Allow\",\n" +
                "            \"Principal\": {\"Service\": \"logging.s3.amazonaws.com
\"},\n" +
                "            \"Action\": [\n" +
                "                \"s3:PutObject\"\n" +
                "            ],\n" +
                "            \"Resource\": \"arn:aws:s3:::" + targetBucketName + "/*
\",\n" +
                "            \"Condition\": {\n" +
                "                \"ArnLike\": {\n" +
                "                    \"aws:SourceArn\": \"arn:aws:s3:::" +
 sourceBucketName + "\"\n" +
                "                },\n" +
                "                \"StringEquals\": {\n" +
                "                    \"aws:SourceAccount\": \"" + sourceAccountId +
 "\"\n" +
                "                }\n" +
                "            }\n" +
                "        }\n" +
                "    ]\n" +
                "}";
        s3Client.putBucketPolicy(b -> b.bucket(targetBucketName).policy(policy));
    }

    // Function to enable server access logging on the source S3 bucket.
    public void enableServerAccessLogging(String sourceBucketName, String
 targetBucketName,
```

```
            String targetPrefix) {
        TargetObjectKeyFormat targetObjectKeyFormat =
 TargetObjectKeyFormat.builder()

 .partitionedPrefix(PartitionedPrefix.builder().partitionDateSource("EventTime").build())
                .build();
        LoggingEnabled loggingEnabled = LoggingEnabled.builder()
                .targetBucket(targetBucketName)
                .targetPrefix(targetPrefix)
                .targetObjectKeyFormat(targetObjectKeyFormat)
                .build();
        BucketLoggingStatus bucketLoggingStatus = BucketLoggingStatus.builder()
                .loggingEnabled(loggingEnabled)
                .build();
        s3Client.putBucketLogging(PutBucketLoggingRequest.builder()
                .bucket(sourceBucketName)
                .bucketLoggingStatus(bucketLoggingStatus)
                .build());
    }

}
```

À l'aide du AWS CLI

Nous vous recommandons de créer un compartiment de journalisation dédié dans chaque compartiment dans Région AWS lequel vous avez des compartiments S3. Ensuite, faites en sorte que les journaux d'accès Amazon S3 soient livrés dans ce compartiment S3. Pour plus d'informations et des exemples, consultez put-bucket-logging dans la référence AWS CLI .

Si le compartiment de destination (cible) utilise le paramètre imposé par le propriétaire du compartiment pour la propriété de l'objet, vous ne pouvez pas définir de compartiment ou d'objet ACLs. Vous ne pouvez pas non plus inclure d'autorisations de destination (cible) dans votre PutBucketLoggingconfiguration. Vous devez utiliser une politique de compartiment pour accorder l'accès au principal du service de journalisation (`logging.s3.amazonaws.com`). Pour plus d'informations, consultez Autorisations de diffusion de journaux.

Example – Activer des journaux d'accès avec cinq compartiments répartis dans deux Régions

Dans cet exemple, vous disposez des cinq compartiments suivants :

- *amzn-s3-demo-source-bucket*-us-east-1

- *amzn-s3-demo-source-bucket1*-us-east-1
- *amzn-s3-demo-source-bucket2*-us-east-1
- *amzn-s3-demo-bucket1*-us-west-2
- *amzn-s3-demo-bucket2*-us-west-2

> **Note**
>
> La dernière étape de la procédure suivante fournit des exemples de scripts bash que vous pouvez utiliser pour créer vos compartiments de journalisation et activer la journalisation des accès au serveur sur ces compartiments. Pour utiliser ces scripts, vous devez créer les fichiers `policy.json` et `logging.json`, comme décrit dans la procédure suivante.

1. Créez deux compartiments de destination de journalisation dans les régions USA Ouest (Oregon) et USA Est (Virginie du Nord) et donnez-leur les noms suivants :
   - *amzn-s3-demo-destination-bucket*-logs-us-east-1
   - *amzn-s3-demo-destination-bucket1*-logs-us-west-2
2. Plus tard dans ces étapes, vous activerez la journalisation des accès au serveur comme suit :
   - *amzn-s3-demo-source-bucket*-us-east-1 consigne dans le compartiment S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 avec le préfixe *amzn-s3-demo-source-bucket*-us-east-1.
   - *amzn-s3-demo-source-bucket1*-us-east-1 consigne dans le compartiment S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 avec le préfixe *amzn-s3-demo-source-bucket1*-us-east-1.
   - *amzn-s3-demo-source-bucket2*-us-east-1 consigne dans le compartiment S3 *amzn-s3-demo-destination-bucket*-logs-us-east-1 avec le préfixe *amzn-s3-demo-source-bucket2*-us-east-1.
   - *amzn-s3-demo-bucket1*-us-west-2 consigne dans le compartiment S3 *amzn-s3-demo-destination-bucket1*-logs-us-west-2 avec le préfixe *amzn-s3-demo-bucket1*-us-west-2.
   - *amzn-s3-demo-bucket2*-us-west-2 consigne dans le compartiment S3 *amzn-s3-demo-destination-bucket1*-logs-us-west-2 avec le préfixe *amzn-s3-demo-bucket2*-us-west-2.

3. Pour chaque compartiment de journalisation de destination, accordez des autorisations pour la livraison des journaux d'accès au serveur à l'aide d'une liste ACL de compartiment ou d'une politique de compartiment :

   - Mettre à jour la politique de compartiment (recommandé) : pour accorder des autorisations au principal du service de journalisation, utilisez la commande `put-bucket-policy` suivante. Remplacez *`amzn-s3-demo-destination-bucket`*`-logs` par le nom de votre compartiment de destination.

     ```
     aws s3api put-bucket-policy --bucket amzn-s3-demo-destination-bucket-logs --
     policy file://policy.json
     ```

     `Policy.json` est un document JSON dans le dossier actuel qui contient la politique de compartiment suivante. Pour utiliser cette politique de compartiment, remplacez *`user input placeholders`* par vos propres informations. Dans la politique suivante, *`amzn-s3-demo-destination-bucket-logs`* est le compartiment de destination où les journaux des accès au serveur seront livrés, et *`amzn-s3-demo-source-bucket`* est le compartiment source. *`SOURCE-ACCOUNT-ID`* est le Compte AWS qui possède le compartiment source.

     JSON

     ```
     {
         "Version": "2012-10-17",
         "Statement": [
             {
                 "Sid": "S3ServerAccessLogsPolicy",
                 "Effect": "Allow",
                 "Principal": {
                     "Service": "logging.s3.amazonaws.com"
                 },
                 "Action": [
                     "s3:PutObject"
                 ],
                 "Resource": "arn:aws:s3:::amzn-s3-demo-destination-bucket-logs/
     *",
                 "Condition": {
                     "ArnLike": {
                         "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-source-
     bucket"
                     },
     ```

```
                "StringEquals": {
                    "aws:SourceAccount": "SOURCE-ACCOUNT-ID"
                }
            }
        }
    ]
}
```

- Mettre à jour la liste ACL de compartiment : pour accorder des autorisations au groupe de livraison des journaux S3, utilisez la commande `put-bucket-acl` suivante. Remplacez *amzn-s3-demo-destination-bucket-logs* par le nom de votre compartiment de destination (cible).

```
aws s3api put-bucket-acl --bucket amzn-s3-demo-destination-bucket-logs  --
grant-write URI=http://acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp
 URI=http://acs.amazonaws.com/groups/s3/LogDelivery
```

4. Créez ensuite un fichier `logging.json` contenant votre configuration de journalisation (en vous basant sur l'un des trois exemples suivants). Après avoir créé le fichier `logging.json`, vous pouvez appliquer la configuration de journalisation à l'aide de la commande `put-bucket-logging` suivante. Remplacez *amzn-s3-demo-destination-bucket-logs* par le nom de votre compartiment de destination (cible).

```
aws s3api put-bucket-logging --bucket amzn-s3-demo-destination-bucket-logs --
bucket-logging-status file://logging.json
```

> **Note**
>
> Au lieu d'utiliser cette commande `put-bucket-logging` pour appliquer la configuration de journalisation sur chaque compartiment de destination, vous pouvez utiliser l'un des scripts bash fournis à l'étape suivante. Pour utiliser ces scripts, vous devez créer les fichiers `policy.json` et `logging.json`, comme décrit dans cette procédure.

Le fichier `logging.json` est un document JSON situé dans le dossier actuel, qui contient votre configuration de journalisation. Si un compartiment de destination utilise le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets, votre configuration de journalisation ne peut pas contenir d'octrois de destination (cibles). Pour plus d'informations, consultez Autorisations de diffusion de journaux.

Example : **`logging.json`** sans octrois de destination (cibles)

L'exemple de fichier `logging.json` suivant ne contient pas d'octrois de destination (cibles). Par conséquent, vous pouvez appliquer cette configuration à un compartiment de destination (cible) qui utilise le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets.

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/"
     }
 }
```

Example : **`logging.json`** avec des octrois de destination (cibles)

L'exemple de fichier `logging.json` suivant contient des octrois de destination (cibles).

Si le compartiment de destination utilise le paramètre Appliqué par le propriétaire du compartiment pour Propriété d'objets, vous ne pouvez pas inclure d'octrois de destination (cibles) dans votre configuration PutBucketLogging. Pour de plus amples informations, veuillez consulter Autorisations de diffusion de journaux.

```
{
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/",
        "TargetGrants": [
             {
                "Grantee": {
                    "Type": "AmazonCustomerByEmail",
```

```
                    "EmailAddress": "user@example.com"
                },
                "Permission": "FULL_CONTROL"
            }
        ]
    }
}
```

Valeurs des bénéficiaires

Vous pouvez spécifier la personne (bénéficiaire) à laquelle vous attribuez les droits d'accès (en utilisant les éléments de demande) de la manière suivante :

- Par le numéro d'identification de la personne :

  ```
  {
    "Grantee": {
      "Type": "CanonicalUser",
      "ID": "ID",
      "DisplayName": "GranteesEmail"
    }
  }
  ```

  `DisplayName`est facultatif et est ignoré dans la demande.

- Par adresse e-mail :

  ```
  {
    "Grantee": {
      "Type": "AmazonCustomerByEmail",
      "EmailAddress": "username@example.com"
    }
  }
  ```

  Le bénéficiaire est résolu à la `CanonicalUser` et, dans une réponse à une `GetObjectAcl` demande, apparaît sous la forme de`CanonicalUser`.

> **Note**
>
> L'utilisation d'adresses e-mail pour spécifier un bénéficiaire n'est prise en charge que dans certains Régions AWS cas. Pour plus d'informations, consultez Grantee dans la Référence d'API Amazon S3.

- Par URI :

```
{
  "Grantee": {
    "Type": "Group",
    "URI": "http://acs.amazonaws.com/groups/global/AuthenticatedUsers"
  }
}
```

Example : **`logging.json`** avec le format de clé d'objet journal défini sur Heure de l'événement S3

Le fichier `logging.json` suivant remplace le format de clé d'objet journal par l'heure de l'événement S3. Pour plus d'informations sur la définition du format de clé d'objet journal, consultez the section called "Comment activer la livraison des journaux ?".

```
  {
    "LoggingEnabled": {
        "TargetBucket": "amzn-s3-demo-destination-bucket-logs",
        "TargetPrefix": "amzn-s3-demo-destination-bucket/",
        "TargetObjectKeyFormat": {
            "PartitionedPrefix": {
                "PartitionDateSource": "EventTime"
            }
         }
    }
}
```

5. Utilisez l'un des scripts bash suivants pour ajouter la journalisation des accès pour tous les compartiments dans votre compte. Remplacez *amzn-s3-demo-destination-bucket-logs*

par le nom de votre compartiment de destination (cible) et remplacez *us-west-2* par le nom de la région où se trouvent vos compartiments.

> **Note**
>
> Ce script fonctionne uniquement si tous vos compartiments se trouvent dans la même région. Si vous disposez de compartiments dans plusieurs Régions, vous devez adapter le script.

Example — Accordez l'accès avec des stratégies de compartiment et ajoutez la journalisation pour les compartiments de votre compte

```
loggingBucket='amzn-s3-demo-destination-bucket-logs'
region='us-west-2'


# Create the logging bucket.
aws s3 mb s3://$loggingBucket --region $region

aws s3api put-bucket-policy --bucket $loggingBucket --policy file://policy.json

# List the buckets in this account.
buckets="$(aws s3 ls | awk '{print $3}')"

# Put a bucket logging configuration on each bucket.
for bucket in $buckets
    do
      # This if statement excludes the logging bucket.
      if [ "$bucket" == "$loggingBucket" ] ; then
          continue;
      fi
      printf '{
        "LoggingEnabled": {
          "TargetBucket": "%s",
          "TargetPrefix": "%s/"
      }
    }' "$loggingBucket" "$bucket"  > logging.json
    aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
    echo "$bucket done"
```

```
  done

  rm logging.json

  echo "Complete"
```

Example — Accordez l'accès avec un bucket ACLs et ajoutez une journalisation pour les buckets de votre compte

```
  loggingBucket='amzn-s3-demo-destination-bucket-logs'
  region='us-west-2'


  # Create the logging bucket.
  aws s3 mb s3://$loggingBucket --region $region

  aws s3api put-bucket-acl --bucket $loggingBucket --grant-write URI=http://
acs.amazonaws.com/groups/s3/LogDelivery --grant-read-acp URI=http://
acs.amazonaws.com/groups/s3/LogDelivery

  # List the buckets in this account.
  buckets="$(aws s3 ls | awk '{print $3}')"

  # Put a bucket logging configuration on each bucket.
  for bucket in $buckets
      do
        # This if statement excludes the logging bucket.
        if [ "$bucket" == "$loggingBucket" ] ; then
            continue;
        fi
        printf '{
          "LoggingEnabled": {
            "TargetBucket": "%s",
            "TargetPrefix": "%s/"
        }
      }' "$loggingBucket" "$bucket"  > logging.json
      aws s3api put-bucket-logging --bucket $bucket --bucket-logging-status file://
logging.json
      echo "$bucket done"
  done

  rm logging.json
```

```
echo "Complete"
```

Vérification de votre configuration des journaux d'accès au serveur

Après avoir activé la journalisation des accès au serveur, effectuez les étapes suivantes :

- Accédez au compartiment de destination et vérifiez que les fichiers journaux sont livrés. Une fois les journaux d'accès configurés, Amazon S3 commence immédiatement à capturer les demandes et à les journaliser. Toutefois, la livraison des journaux dans le compartiment de destination peut prendre quelques heures. Pour plus d'informations, consultez the section called "Les changements de statut de la journalisation des compartiments prennent effet au fil du temps" et the section called "Livraison des journaux du serveur dans la mesure du possible".

  Vous pouvez également vérifier automatiquement la livraison des journaux en utilisant les métriques de demande Amazon S3 et en configurant des CloudWatch alarmes Amazon pour ces métriques. Pour de plus amples informations, veuillez consulter Surveillance des métriques avec Amazon CloudWatch.
- Vérifiez que vous êtes en mesure d'ouvrir et de lire le contenu des fichiers journaux.

Pour obtenir des informations sur la résolution des problèmes de journalisation des accès au serveur, consultez Résolution des problèmes de journalisation des accès au serveur.

Format des journaux d'accès au serveur Amazon S3

La journalisation des accès au serveur fournit des enregistrements détaillés des demandes soumises à un compartiment Amazon S3. Vous pouvez utiliser les journaux d'accès au serveur dans les buts suivants :

- Réalisation d'audits de sécurité et d'accès
- Apprendre à connaître votre clientèle
- Comprendre votre facture Amazon S3

Cette section décrit le format et d'autres détails des fichiers journaux d'accès au serveur Amazon S3.

Les fichiers journaux d'accès au serveur consistent en une séquence d'enregistrements de journaux délimités par un retour à la ligne. Chaque enregistrement de journaux représente une demande et consiste en des champs séparés par des espaces.

Voici un exemple de journal composé de cinq enregistrements.

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 3E57427F3EXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 - 113 - 7 -
 "-" "S3Console/0.4" - s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/
XV/VLi31234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-demo-bucket1.s3.us-
west-1.amazonaws.com TLSV1.2 arn:aws:s3:us-west-1:123456789012:accesspoint/example-AP
 Yes
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 891CE47D2EXAMPLE
 REST.GET.LOGGING_STATUS - "GET /amzn-s3-demo-bucket1?logging HTTP/1.1" 200 -
 242 - 11 - "-" "S3Console/0.4" - 9vKBE6vMhrNiWHZmb2L0mXOcqPGzQOI5XLnCtZNPxev+Hf
+7tpT6sxDwDty4LHBUOZJG96N1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:00:38 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be A1206F460EXAMPLE
 REST.GET.BUCKETPOLICY - "GET /amzn-s3-demo-bucket1?policy HTTP/1.1" 404
 NoSuchBucketPolicy 297 - 38 - "-" "S3Console/0.4" - BNaBsXZQQDbssi6xMBdBU2sLt
+Yf5kZDmeBUP35sFoKa3sLLeMC78iwEIWxs99CRUrbS4n11234= SigV4 ECDHE-RSA-AES128-GCM-SHA256
 AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - Yes
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:00 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be 7B4A0FABBEXAMPLE
 REST.GET.VERSIONING - "GET /amzn-s3-demo-bucket1?versioning HTTP/1.1" 200 -
 113 - 33 - "-" "S3Console/0.4" - Ke1bUcazaN1jWuUlPJaxF64cQVpUEhoZKEG/hmy/gijN/
I1DeWqDfFvnpybfEseEME/u7ME1234= SigV4 ECDHE-RSA-AES128-GCM-SHA256 AuthHeader amzn-s3-
demo-bucket1.s3.us-west-1.amazonaws.com TLSV1.2 - -
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 amzn-s3-demo-bucket1 [06/Feb/2019:00:01:57 +0000] 192.0.2.3
 79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
 DD6CC733AEXAMPLE REST.PUT.OBJECT s3-dg.pdf "PUT /amzn-s3-demo-bucket1/
s3-dg.pdf HTTP/1.1" 200 - - 4406583 41754 28 "-" "S3Console/0.4" -
 10S62Zv81kBW7BB6SX4XJ48o6kpcl6LPwEoizZQQxJd5qDSCTLX0TgS37kYUBKQW3+bPdrg1234= SigV4
 ECDHE-RSA-AES128-SHA AuthHeader amzn-s3-demo-bucket1.s3.us-west-1.amazonaws.com
 TLSV1.2 - Yes
```

> **Note**
>
> Tous les champs peuvent être configurés sur - pour indiquer que les données étaient inconnues ou indisponibles, ou que le champ ne s'appliquait pas à cette demande.

Rubriques

- Champs d'enregistrement des journaux
- Journalisation supplémentaire les opérations de copie
- Informations personnalisées des journaux d'accès
- Remarques de programmation relatives au format étendu des journaux d'accès au serveur

Champs d'enregistrement des journaux

La liste suivante décrit les champs de l'enregistrement des journaux.

Propriétaire du compartiment

L'ID d'utilisateur canonique du propriétaire du compartiment source. L'ID utilisateur canonique est une autre forme de l' Compte AWS ID. Pour plus d'informations sur l'ID d'utilisateur canonique, consultez Identificateurs de Compte AWS dans Références générales AWS. Pour savoir comment trouver l'ID d'utilisateur canonique de votre compte, consultez Identification de l'ID d'utilisateur canonique de votre Compte AWS.

Exemple d'entrée

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Compartiment

Le nom du compartiment sur lequel la demande a été traitée. Si le système reçoit une demande erronée et ne peut pas déterminer le compartiment, la demande n'apparaît sur aucun journal d'accès au serveur.

Exemple d'entrée

```
amzn-s3-demo-bucket1
```

Heure

Heure à laquelle la demande a été reçue. Ces dates et heures sont exprimées en heure UTC (temps universel coordonné). Le format, en utilisant terminologie `strftime()`, est le suivant : `[%d/%b/%Y:%H:%M:%S %z]`

Exemple d'entrée

```
[06/Feb/2019:00:00:38 +0000]
```

Adresse IP distante

L'adresse IP apparente du demandeur. Les proxys et pare-feu intermédiaires doivent cacher l'adresse IP réelle de la machine à l'origine de la demande.

Exemple d'entrée

```
192.0.2.3
```

Demandeur

ID d'utilisateur canonique du demandeur, ou `-` pour les demandes non authentifiées. Si le demandeur était un utilisateur IAM, ce champ renvoie le nom d'utilisateur IAM du demandeur ainsi Compte AWS que le nom auquel appartient l'utilisateur IAM. Cet identifiant est le même que celui qui est utilisé pour contrôler l'accès.

Exemple d'entrée

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Si le demandeur utilise un rôle endossé, ce champ renvoie le rôle IAM correspondant.

Exemple d'entrée

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

ID de demande

Chaîne de caractères générée par Amazon S3 pour identifier de façon unique chaque demande.

Exemple d'entrée

```
3E57427F33A59F07
```

Opération

L'opération listée ici est déclarée comme `SOAP.operation`, `REST.HTTP_method.resource_type`, `WEBSITE.HTTP_method.resource_type` ou `BATCH.DELETE.OBJECT`, ou `S3.action.resource_type` pour Cycle de vie S3 et journalisation.

Exemple d'entrée

```
REST.PUT.OBJECT
```

Clé

La partie clé (nom de l'objet) de la demande.

Exemple d'entrée

```
/photos/2019/08/puppy.jpg
```

Request-URI

La partie `Request-URI` du message de requête HTTP.

Exemple d'entrée

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar HTTP/1.1"
```

Statut HTTP

Code numérique du statut HTTP de la réponse.

Exemple d'entrée

```
200
```

Code d'erreur

Réponses d'erreur Amazon S3 ou - si aucune erreur ne s'est produite.

Exemple d'entrée

```
NoSuchBucket
```

Octets envoyés

Nombre d'octets de réponse envoyés, hors surcharge de protocole HTTP ou - si zéro.

Exemple d'entrée

```
2662992
```

Taille de l'objet

Taille totale de l'objet en question.

Exemple d'entrée

```
3462992
```

Durée totale

Le nombre de millisecondes (ms) pendant lesquelles la demande était en cours du point de vue du serveur. Cette valeur est mesurée entre la réception de la demande et l'envoi du dernier octet de la réponse. Les mesures effectuées depuis la perspective du client peuvent être plus longues en raison de la latence du réseau.

Exemple d'entrée

```
70
```

Délai de traitement

Le nombre de millisecondes pendant lesquelles Amazon S3 a traité la demande. Cette valeur est mesurée entre la réception du dernier octets de votre demande et l'envoi du premier octet de la réponse.

Exemple d'entrée

```
10
```

Referer

Valeur de l'en-tête du `Referer` HTTP, le cas échéant. Les agents utilisateur HTTP (par exemple, les navigateurs) définissent généralement cet en-tête comme l'URL de la page de liaison ou d'intégration lors d'une demande.

Exemple d'entrée

```
"http://www.example.com/webservices"
```

User-Agent

Valeur de l'en-tête du `User-Agent` HTTP.

Exemple d'entrée

```
"curl/7.15.1"
```

ID de version

L'ID de version dans la demande ou `-` si l'opération n'accepte pas de paramètre `versionId`.

Exemple d'entrée

```
3HL4kqtJvjVBH40Nrjfkd
```

ID de l'hôte

L'ID de la requête étendue `x-amz-id-2` ou Amazon S3.

Exemple d'entrée

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Version de signature

Version de signature, `SigV2` ou `SigV4`, qui a été utilisée pour authentifier la demande ou `-` pour les demandes non authentifiées.

Exemple d'entrée

```
SigV2
```

Suite de chiffrement

Chiffre TLS (Transport Layer Security) négocié pour une requête HTTPS ou `-` pour HTTP.

Exemple d'entrée

```
ECDHE-RSA-AES128-GCM-SHA256
```

Type d'authentification

Type d'authentification de requête utilisé : `AuthHeader` pour les en-têtes d'authentification, `QueryString` pour la chaîne de requête (URL présignée), ou `-` pour les demandes non authentifiées.

Exemple d'entrée

```
AuthHeader
```

En-tête d'hôte

Point de terminaison utilisé pour vous connecter à Amazon S3.

Exemple d'entrée

```
s3.us-west-2.amazonaws.com
```

Certaines régions antérieures prennent en charge les points de terminaison hérités. Vous pouvez voir ces points de terminaison dans les journaux ou AWS CloudTrail journaux d'accès de votre serveur. Pour de plus amples informations, veuillez consulter Points de terminaison hérités. Pour obtenir la liste complète des régions et points de terminaison Amazon S3, consultez Points de terminaison et quotas Amazon S3 dans le Référence générale d'Amazon Web Services.

Version de TLS

Version de protocole TLS (Transport Layer Security) négociée par le client. La valeur est l'une des valeurs suivantes : `TLSv1.1`, `TLSv1.2`, `TLSv1.3` ou `-` si le protocole TLS n'a pas été utilisé.

Exemple d'entrée

```
TLSv1.2
```

ARN de point d'accès

Amazon Resource Name (ARN) du point d'accès de la demande. Si l'ARN du point d'accès est mal formé ou n'est pas utilisé, le champ contient un `-`. Pour plus d'informations sur les points d'accès, consultez Utilisation des points d'accès Amazon S3 pour des compartiments à usage général. Pour plus d'informations ARNs, consultez Amazon Resource Name (ARN) dans le guide de AWS référence.

Exemple d'entrée

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

Une chaîne qui indique si la requête a nécessité une liste de contrôle d'accès (ACL) pour l'autorisation. Si la requête a nécessité un ACL pour l'autorisation, la chaîne est `Yes`. Si vous ACLs n'en avez pas besoin, la chaîne est`-`. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL). Pour plus d'informations sur l'utilisation du `aclRequired` champ pour désactiver ACLs, consultezContrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Exemple d'entrée

```
Yes
```

Journalisation supplémentaire les opérations de copie

Une copie implique une demande `GET` et une demande `PUT`. C'est pourquoi, nous consignons deux enregistrements lors d'une opération de copie. La section précédente décrit les champs liés à la partie `PUT` de l'opération. La liste suivante décrit les champs dans l'enregistrement qui ont trait à la partie `GET` de l'opération de copie.

Propriétaire du compartiment

L'ID d'utilisateur canonique du compartiment qui stocke l'objet en cours de copie. L'ID utilisateur canonique est une autre forme de l' Compte AWS ID. Pour plus d'informations sur l'ID d'utilisateur

canonique, consultez Identificateurs de Compte AWS dans Références générales AWS. Pour savoir comment trouver l'ID d'utilisateur canonique de votre compte, consultez Identification de l'ID d'utilisateur canonique de votre Compte AWS.

Exemple d'entrée

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Compartiment

Nom du compartiment qui stocke l'objet à copier.

Exemple d'entrée

```
amzn-s3-demo-bucket1
```

Heure

Heure à laquelle la demande a été reçue. Ces dates et heures sont exprimées en heure UTC (temps universel coordonné). Le format, en utilisant terminologie `strftime()`, est le suivant : `[%d/%B/%Y:%H:%M:%S %z]`

Exemple d'entrée

```
[06/Feb/2019:00:00:38 +0000]
```

Adresse IP distante

L'adresse IP apparente du demandeur. Les proxys et pare-feu intermédiaires doivent cacher l'adresse IP réelle de la machine à l'origine de la demande.

Exemple d'entrée

```
192.0.2.3
```

Demandeur

ID d'utilisateur canonique du demandeur, ou `-` pour les demandes non authentifiées. Si le demandeur était un utilisateur IAM, ce champ renverra le nom d'utilisateur IAM du demandeur ainsi Utilisateur racine d'un compte AWS que le nom auquel appartient l'utilisateur IAM. Cet identifiant est le même que celui qui est utilisé pour contrôler l'accès.

Exemple d'entrée

```
79a59df900b949e55d96a1e698fbacedfd6e09d98eacf8f8d5218e7cd47ef2be
```

Si le demandeur utilise un rôle endossé, ce champ renvoie le rôle IAM correspondant.

Exemple d'entrée

```
arn:aws:sts::123456789012:assumed-role/roleName/test-role
```

ID de demande

Chaîne de caractères générée par Amazon S3 pour identifier de façon unique chaque demande.

Exemple d'entrée

```
3E57427F33A59F07
```

Opération

L'opération listée ici est déclarée comme `SOAP.`*`operation`*, `REST.`*`HTTP_method`*`.`*`resource_type`*, `WEBSITE.`*`HTTP_method`*`.`*`resource_type`* ou `BATCH.DELETE.OBJECT`.

Exemple d'entrée

```
REST.COPY.OBJECT_GET
```

Clé

La clé (nom de l'objet) de l'objet à copier, ou `-` si l'opération n'accepte pas de paramètre clé.

Exemple d'entrée

```
/photos/2019/08/puppy.jpg
```

Request-URI

La partie `Request-URI` du message de requête HTTP.

Exemple d'entrée

```
"GET /amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-foo=bar"
```

Statut HTTP

Code numérique du statut HTTP de la partie GET de l'opération de copie.

Exemple d'entrée

```
200
```

Code d'erreur

Réponses d'erreur Amazon S3 de la partie GET de l'opération de copie ou - si aucune erreur ne s'est produite.

Exemple d'entrée

```
NoSuchBucket
```

Octets envoyés

Nombre d'octets de réponse envoyés, hors surcharge de protocole HTTP ou - si zéro.

Exemple d'entrée

```
2662992
```

Taille de l'objet

Taille totale de l'objet en question.

Exemple d'entrée

```
3462992
```

Durée totale

Le nombre de millisecondes (ms) pendant lesquelles la demande était en cours du point de vue du serveur. Cette valeur est mesurée entre la réception de la demande et l'envoi du dernier octet de la réponse. Les mesures effectuées depuis la perspective du client peuvent être plus longues en raison de la latence du réseau.

Exemple d'entrée

```
70
```

Délai de traitement

Le nombre de millisecondes pendant lesquelles Amazon S3 a traité la demande. Cette valeur est mesurée entre la réception du dernier octets de votre demande et l'envoi du premier octet de la réponse.

Exemple d'entrée

```
10
```

Referer

Valeur de l'en-tête du `Referer` HTTP, le cas échéant. Les agents utilisateur HTTP (par exemple, les navigateurs) définissent généralement cet en-tête comme l'URL de la page de liaison ou d'intégration lors d'une demande.

Exemple d'entrée

```
"http://www.example.com/webservices"
```

User-Agent

Valeur de l'en-tête du `User-Agent` HTTP.

Exemple d'entrée

```
"curl/7.15.1"
```

ID de version

ID de version de l'objet à copier ou `-` si l'en-tête `x-amz-copy-source` n'a pas spécifié de paramètre `versionId` dans la source de copie.

Exemple d'entrée

```
3HL4kqtJvjVBH40Nrjfkd
```

ID de l'hôte

L'ID de la requête étendue `x-amz-id-2` ou Amazon S3.

Exemple d'entrée

```
s9lzHYrFp76ZVxRcpX9+5cjAnEH2ROuNkd2BHfIa6UkFVdtjf5mKR3/eTPFvsiP/XV/VLi31234=
```

Version de signature

Version de signature, `SigV2` ou `SigV4`, qui a été utilisée pour authentifier la demande ou `-` pour les demandes non authentifiées.

Exemple d'entrée

```
SigV4
```

Suite de chiffrement

Chiffre TLS (Transport Layer Security) négocié pour une requête HTTPS ou `-` pour HTTP.

Exemple d'entrée

```
ECDHE-RSA-AES128-GCM-SHA256
```

Type d'authentification

Type d'authentification de demande utilisé : `AuthHeader` pour les en-têtes d'authentification, `QueryString` pour les chaînes de requête (présignées URLs) ou `-` pour les demandes non authentifiées.

Exemple d'entrée

```
AuthHeader
```

En-tête d'hôte

Point de terminaison utilisé pour vous connecter à Amazon S3.

Exemple d'entrée

```
s3.us-west-2.amazonaws.com
```

Certaines régions antérieures prennent en charge les points de terminaison hérités. Vous pouvez voir ces points de terminaison dans les journaux ou AWS CloudTrail journaux d'accès de votre serveur. Pour de plus amples informations, veuillez consulter Points de terminaison hérités. Pour obtenir la liste complète des régions et points de terminaison Amazon S3, consultez Points de terminaison et quotas Amazon S3 dans le Référence générale d'Amazon Web Services.

Version de TLS

Version de protocole TLS (Transport Layer Security) négociée par le client. La valeur est l'une des valeurs suivantes : `TLSv1.1`, `TLSv1.2`, `TLSv1.3` ou `-` si le protocole TLS n'a pas été utilisé.

Exemple d'entrée

```
TLSv1.2
```

ARN de point d'accès

Amazon Resource Name (ARN) du point d'accès de la demande. Si l'ARN du point d'accès est mal formé ou n'est pas utilisé, le champ contient un `-`. Pour plus d'informations sur les points d'accès, consultez Utilisation des points d'accès Amazon S3 pour des compartiments à usage général. Pour plus d'informations ARNs, consultez Amazon Resource Name (ARN) dans le guide de AWS référence.

Exemple d'entrée

```
arn:aws:s3:us-east-1:123456789012:accesspoint/example-AP
```

aclRequired

Une chaîne qui indique si la requête a nécessité une liste de contrôle d'accès (ACL) pour l'autorisation. Si la requête a nécessité un ACL pour l'autorisation, la chaîne est `Yes`. Si vous ACLs n'en avez pas besoin, la chaîne est`-`. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL). Pour plus d'informations sur l'utilisation du `aclRequired` champ pour désactiver ACLs, consultezContrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Exemple d'entrée

```
Yes
```

Informations personnalisées des journaux d'accès

Vous pouvez inclure des informations personnalisées à stocker dans le journal d'accès pour une demande. Pour ce faire, ajoutez un paramètre de chaîne de requête personnalisé à l'URL utilisée. Amazon S3 ignore les paramètres de la chaîne de requête qui commencent par `x-`, mais inclut ces derniers dans les enregistrements des journaux d'accès pour la demande dans le champ `Request-URI`.

Par exemple, une demande `GET` pour `"s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg?x-user=johndoe"` fonctionne de la même manière que la demande pour `"s3.amazonaws.com/amzn-s3-demo-bucket1/photos/2019/08/puppy.jpg"`, sauf que la chaîne `"x-user=johndoe"` est incluse dans le champ `Request-URI` de l'enregistrement de journal associé. Cette fonctionnalité est uniquement disponible dans l'interface REST.

Remarques de programmation relatives au format étendu des journaux d'accès au serveur

Parfois, nous pouvons étendre le format d'enregistrement du journal d'accès en ajoutant de nouveaux champs à la fin de chaque ligne. Par conséquent, assurez-vous que tout votre code qui analyse les journaux d'accès au serveur peut gérer les champs de suivi qu'il pourrait ne pas comprendre.

Suppression des fichiers journaux Amazon S3

Un compartiment Amazon S3 dont la journalisation des accès au serveur est activée peut accumuler un grand nombre de journaux au fil du temps. L'application peut avoir besoin de ces journaux d'accès pendant une période donnée après leur création, après quoi vous pourrez les supprimer. Vous pouvez utiliser la configuration de cycle de vie Amazon S3 pour définir des règles afin qu'Amazon S3 mette automatiquement ces objets en file d'attente de suppression à la fin de leur vie.

Vous pouvez définir une configuration de cycle de vie pour un sous-ensemble d'objets dans votre compartiment S3 à l'aide d'un préfixe partagé. Si vous spécifiez un préfixe dans la configuration de la journalisation des accès au serveur, vous pouvez configurer une règle de configuration du cycle de vie pour supprimer les objets du journal qui ont ce préfixe.

Par exemple, supposons que vos objets journaux aient le préfixe `logs/`. Vous pouvez définir une règle de configuration de cycle de vie pour supprimer tous les objets du compartiment dotés du préfixe `logs/` après une période de temps spécifiée.

Pour en savoir plus sur la configuration du cycle de vie, consultez Gestion du cycle de vie des objets.

Pour plus d'informations sur la journalisation des accès au serveur, consultez Enregistrement de demandes avec journalisation des accès au serveur.

Utilisation des journaux d'accès au serveur Amazon S3 pour identifier des demandes

Vous pouvez identifier des demandes Amazon S3 à l'aide des journaux d'accès au serveur Amazon S3.

> **Note**
>
> - Pour identifier les demandes Amazon S3, nous vous recommandons d'utiliser AWS CloudTrail des événements de données plutôt que des journaux d'accès au serveur Amazon S3. CloudTrail les événements de données sont plus faciles à configurer et contiennent davantage d'informations. Pour de plus amples informations, veuillez consulter Identification des demandes Amazon S3 à l'aide de CloudTrail.
> - Selon le nombre de demandes d'accès que vous recevez, l'analyse de vos journaux peut nécessiter plus de ressources ou de temps que l'utilisation d'événements de CloudTrail données.

Rubriques

- Interrogation des journaux d'accès pour les demandes à l'aide d'Amazon Athena
- Identification des demandes Signature Version 2 à l'aide des journaux d'accès Amazon S3
- Identification des demandes d'accès aux objets à l'aide des journaux d'accès Amazon S3

Interrogation des journaux d'accès pour les demandes à l'aide d'Amazon Athena

Vous pouvez identifier les demandes Amazon S3 à l'aide des journaux d'accès Amazon S3 en utilisant Amazon Athena.

Amazon S3 stocke les journaux d'accès au serveur en tant qu'objets dans un compartiment S3. Il est souvent plus facile d'utiliser un outil capable d'analyser les journaux dans Amazon S3. Athena prend en charge l'analyse des objets S3 et ne peut pas être utilisé pour interroger les journaux d'accès Amazon S3.

Example

L'exemple suivant montre comment vous pouvez interroger les journaux d'accès au serveur Amazon S3 dans Amazon Athena. Remplacez les *user input placeholders* utilisés dans les exemples suivants par vos propres informations.

> **Note**
>
> Pour spécifier un emplacement Amazon S3 dans une requête Athena, vous devez fournir un URI S3 pour le compartiment où vos journaux sont livrés. Cet URI doit inclure le nom et le préfixe du compartiment au format suivant : `s3://`*amzn-s3-demo-bucket1-logs/prefix*`/`

1. Ouvrez la console à l'adresse https://console.aws.amazon.com/athena/.
2. Dans l'Éditeur de requête, exécutez une commande similaire à ce qui suit. Remplacez *s3_access_logs_db* par le nom que vous souhaitez donner à votre base de données.

   ```
   CREATE DATABASE s3_access_logs_db
   ```

   > **Note**
   >
   > Il est recommandé de créer la base de données au même endroit Région AWS que votre compartiment S3.

3. Dans l'Éditeur de requête, exécutez une commande similaire à ce qui suit pour créer un schéma de table dans la base de données que vous avez créée à l'étape 2. Remplacez *s3_access_logs_db.mybucket_logs* par le nom que vous souhaitez donner à votre table. Les valeurs de type de données `STRING` et `BIGINT` sont les propriétés des journaux d'accès. Vous pouvez interroger ces propriétés dans Athena. Pour `LOCATION`, saisissez le compartiment S3 et le préfixe du chemin comme notés précédemment.

   Date-based partitioning

   ```
   CREATE EXTERNAL TABLE s3_access_logs_db.mybucket_logs(
    `bucketowner` STRING,
    `bucket_name` STRING,
    `requestdatetime` STRING,
    `remoteip` STRING,
   ```

```
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
  `turnaroundtime` STRING,
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING,
  `accesspointarn` STRING,
  `aclrequired` STRING)
 PARTITIONED BY (
    `timestamp` string)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
  ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
  ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
  ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://bucket-name/prefix-name/account-id/region/source-bucket-name/'
  TBLPROPERTIES (
   'projection.enabled'='true',
   'projection.timestamp.format'='yyyy/MM/dd',
   'projection.timestamp.interval'='1',
   'projection.timestamp.interval.unit'='DAYS',
   'projection.timestamp.range'='2024/01/01,NOW',
   'projection.timestamp.type'='date',
```

```
  'storage.location.template'='s3://bucket-name/prefix-name/account-id/region/
source-bucket-name/${timestamp}')
```

Non-date-based partitioning

```
CREATE EXTERNAL TABLE `s3_access_logs_db.mybucket_logs`(
  `bucketowner` STRING,
  `bucket_name` STRING,
  `requestdatetime` STRING,
  `remoteip` STRING,
  `requester` STRING,
  `requestid` STRING,
  `operation` STRING,
  `key` STRING,
  `request_uri` STRING,
  `httpstatus` STRING,
  `errorcode` STRING,
  `bytessent` BIGINT,
  `objectsize` BIGINT,
  `totaltime` STRING,
  `turnaroundtime` STRING,
  `referrer` STRING,
  `useragent` STRING,
  `versionid` STRING,
  `hostid` STRING,
  `sigv` STRING,
  `ciphersuite` STRING,
  `authtype` STRING,
  `endpoint` STRING,
  `tlsversion` STRING,
  `accesspointarn` STRING,
  `aclrequired` STRING)
ROW FORMAT SERDE
  'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
  'input.regex'='([^ ]*) ([^ ]*) \\[(.*?)\\] ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) (-|[0-9]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) (\"[^\"]*\"|-) ([^ ]*)(?: ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*) ([^ ]*)
 ([^ ]*) ([^ ]*) ([^ ]*))?.*$')
STORED AS INPUTFORMAT
  'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
```

```
  'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
  's3://amzn-s3-demo-bucket1-logs/prefix/'
```

4. Dans le volet de navigation, sous Database (Base de données), choisissez votre base de données.
5. Sous Tables, choisissez Aperçu de la table en regard du nom de votre table.

   Dans le volet Results (Résultats), vous devriez voir apparaître les données des journaux d'accès au serveur, par exemple `bucketowner`, `bucket`, `requestdatetime`, etc. Ceci signifie que vous avez correctement créé la table Athena. Vous pouvez désormais interroger les journaux d'accès au serveur Amazon S3.

Example – Afficher qui a supprimé un objet et quand (horodatage, adresse IP et utilisateur IAM)

```
SELECT requestdatetime, remoteip, requester, key
FROM s3_access_logs_db.mybucket_logs
WHERE key = 'images/picture.jpg' AND operation like '%DELETE%';
```

Example – Afficher toutes les opérations effectuées par un utilisateur IAM

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE requester='arn:aws:iam::123456789123:user/user_name';
```

Example – Afficher toutes les opérations effectuées sur un objet au cours d'une période spécifique

```
SELECT *
FROM s3_access_logs_db.mybucket_logs
WHERE Key='prefix/images/picture.jpg'
    AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
    BETWEEN parse_datetime('2017-02-18:07:00:00','yyyy-MM-dd:HH:mm:ss')
    AND parse_datetime('2017-02-18:08:00:00','yyyy-MM-dd:HH:mm:ss');
```

Example — afficher la quantité de données transférées vers une adresse IP donnée au cours d'une période

```
SELECT coalesce(SUM(bytessent), 0) AS bytessenttotal
FROM s3_access_logs_db.mybucket_logs
WHERE remoteip='192.0.2.1'
AND parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-06-01','yyyy-MM-dd')
AND parse_datetime('2022-07-01','yyyy-MM-dd');
```

Example — Trouve IDs les requêtes contenant des erreurs HTTP 5xx sur une période donnée

```
SELECT requestdatetime, key, httpstatus, errorcode, requestid, hostid
FROM s3_access_logs_db.mybucket_logs
WHERE httpstatus like '5%' AND timestamp
BETWEEN '2024/01/29'
AND '2024/01/30'
```

> **Note**
>
> Pour réduire le temps de conservation de vos journaux, vous pouvez créer une configuration de cycle de vie S3 pour votre compartiment de journaux d'accès au serveur. Créez des règles de configuration de cycle de vie pour supprimer régulièrement les fichiers journaux. Cela permet de réduire la quantité de données analysées par Athena pour chaque requête. Pour plus d'informations, consultez Définition d'une configuration du cycle de vie S3 sur un compartiment.

Identification des demandes Signature Version 2 à l'aide des journaux d'accès Amazon S3

La prise en charge d'Amazon S3 pour Signature Version 2 sera désactivée (obsolète). Après cela, Amazon S3 n'acceptera plus les demandes utilisant Signature Version 2, et toutes les demandes devront utiliser le processus de signature Signature Version 4. Vous pouvez identifier les demandes d'accès avec Signature Version 2 en utilisant les journaux d'accès Amazon S3.

> **Note**
>
> Pour identifier les demandes Signature version 2, nous vous recommandons d'utiliser AWS CloudTrail des événements de données plutôt que des journaux d'accès au serveur Amazon S3. CloudTrail les événements de données sont plus faciles à configurer et contiennent plus d'informations que les journaux d'accès au serveur. Pour de plus amples informations, veuillez consulter Identification des demandes Amazon S3 Signature version 2 à l'aide de CloudTrail.

Example – Afficher tous les demandeurs qui envoient du trafic Signature Version 2

```
SELECT requester, sigv, Count(sigv) as sigcount
FROM s3_access_logs_db.mybucket_logs
GROUP BY requester, sigv;
```

Identification des demandes d'accès aux objets à l'aide des journaux d'accès Amazon S3

Vous pouvez utiliser des requêtes sur les journaux d'accès au serveur Amazon S3 pour identifier les demandes d'accès aux objets Amazon S3, pour des opérations telles que GET, PUT et DELETE, et découvrir plus d'informations sur ces demandes.

L'exemple de requête Amazon Athena suivant montre comment obtenir toutes les demandes d'objet PUT pour Amazon S3 à partir d'un journal d'accès au serveur.

Example — afficher tous les demandeurs qui envoient des demandes d'objets **PUT** au cours d'une période donnée

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.PUT.OBJECT' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

L'exemple de requête Amazon Athena suivant montre comment obtenir toutes les demandes d'objet GET pour Amazon S3 à partir du journal d'accès au serveur.

Example — afficher tous les demandeurs qui envoient des demandes d'objets **GET** au cours d'une période donnée

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db
WHERE operation='REST.GET.OBJECT' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

L'exemple de requête Amazon Athena suivant montre comment obtenir toutes les demandes anonymes vers vos compartiments S3 à partir du journal d'accès du serveur.

Example — afficher tous les demandeurs anonymes qui adressent des demandes à un compartiment au cours d'une période donnée

```
SELECT bucket_name, requester, remoteip, key, httpstatus, errorcode, requestdatetime
FROM s3_access_logs_db.mybucket_logs
WHERE requester IS NULL AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2019-07-01:00:42:42','yyyy-MM-dd:HH:mm:ss')
AND
parse_datetime('2019-07-02:00:42:42','yyyy-MM-dd:HH:mm:ss')
```

La requête Amazon Athena suivante montre comment identifier toutes les requêtes adressées à vos compartiments S3 qui ont nécessité une liste de contrôle d'accès (ACL) pour l'autorisation. Vous pouvez utiliser ces informations pour migrer ces autorisations ACL vers les politiques de compartiment appropriées et les désactiver ACLs. Après avoir créé ces politiques de compartiment, vous pouvez les désactiver ACLs pour ces compartiments. Pour plus d'informations sur la désactivation ACLs, consultezConditions préalables à la désactivation ACLs.

Example — identifiez toutes les demandes qui ont nécessité un ACL pour l'autorisation.

```
SELECT bucket_name, requester, key, operation, aclrequired, requestdatetime
FROM s3_access_logs_db
```

```
WHERE aclrequired = 'Yes' AND
parse_datetime(requestdatetime,'dd/MMM/yyyy:HH:mm:ss Z')
BETWEEN parse_datetime('2022-05-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
AND parse_datetime('2022-08-10:00:00:00','yyyy-MM-dd:HH:mm:ss')
```

Note

- Vous pouvez modifier la plage de dates en fonction de vos besoins.
- Ces exemples de requêtes peuvent aussi s'avérer utiles pour surveiller la sécurité. Vous pouvez vérifier les résultats pour les appels `PutObject` ou `GetObject` depuis des adresses IP ou des demandeurs inattendus ou non autorisés et pour identifier les demandes anonymes adressées à vos compartiments.
- Cette requête ne récupère d'informations qu'à partir du moment où l'enregistrement a été activé.
- Si vous utilisez AWS CloudTrail des journaux, consultezIdentification de l'accès aux objets S3 en utilisant CloudTrail.

Résolution des problèmes de journalisation des accès au serveur

Les rubriques suivantes peuvent vous aider à résoudre les problèmes que vous êtes susceptible de rencontrer lors de la configuration de la journalisation avec Amazon S3.

Rubriques

- Messages d'erreur courants lors de la configuration de la journalisation
- Dépannage des échecs de livraison

Messages d'erreur courants lors de la configuration de la journalisation

Les messages d'erreur courants suivants peuvent apparaître lorsque vous activez la journalisation via AWS Command Line Interface (AWS CLI) et AWS SDKs :

Erreur : la journalisation entre localisations S3 n'est pas autorisée

Si le compartiment de destination (également appelé compartiment cible) se trouve dans une région différente de celle du compartiment source, une erreur La journalisation entre localisations S3

n'est pas autorisée se produit. Pour résoudre cette erreur, assurez-vous que le compartiment de destination configuré pour recevoir les journaux d'accès se trouve dans le même Région AWS compartiment Compte AWS que le compartiment source.

Erreur : le propriétaire du compartiment à journaliser et celui du compartiment cible doivent être identiques

Lorsque vous activez la journalisation des accès au serveur, cette erreur se produit si le compartiment de destination spécifié appartient à un compte différent. Pour résoudre cette erreur, assurez-vous que le compartiment de destination se trouve dans le même compartiment Compte AWS que le compartiment source.

> **Note**
>
> Nous vous recommandons de choisir un compartiment de destination différent du compartiment source. Lorsque le compartiment source et le compartiment de destination sont identiques, des journaux supplémentaires sont créés pour les journaux qui sont écrits dans le compartiment, ce qui peut augmenter votre facture de stockage. Ces journaux supplémentaires peuvent également rendre difficile de trouver des journaux spécifiques. Pour simplifier la gestion des journaux, nous vous recommandons d'enregistrer les journaux d'accès dans un autre compartiment. Pour plus d'informations, consultez the section called "Comment activer la livraison des journaux ?".

Erreur : le compartiment cible pour la journalisation n'existe pas

Le compartiment de destination doit exister avant de définir la configuration. Cette erreur indique que le compartiment de destination n'existe pas ou est introuvable. Assurez-vous que le nom du compartiment est correctement orthographié, puis réessayez.

Erreur : les accords cibles ne sont pas autorisés pour les compartiments appliqués par le propriétaire du compartiment

Cette erreur indique que le compartiment de destination utilise le paramètre Propriétaire du compartiment appliqué pour la propriété des objets S3. Le paramètre Propriétaire du compartiment appliqué ne prend pas en charge les octrois de destination (cibles). Pour plus d'informations, consultez Autorisations de diffusion de journaux.

Dépannage des échecs de livraison

Pour éviter les problèmes de journalisation des accès au serveur, veillez à suivre les bonnes pratiques suivantes :

- Le groupe de livraison des journaux S3 dispose d'un accès en écriture au compartiment de destination : le groupe de livraison des journaux S3 fournit des journaux d'accès au serveur vers le compartiment de destination. Une politique de compartiment ou une liste de contrôle d'accès (ACL) peuvent être utilisées pour accorder l'accès en écriture au compartiment de destination. Toutefois, nous vous recommandons d'utiliser une politique de compartiment plutôt qu'une liste ACL. Pour plus d'informations sur la manière d'accorder l'accès en écriture à votre compartiment de destination, consultez Autorisations de diffusion de journaux.

  > **Note**
  >
  > Si le compartiment de destination utilise le paramètre Propriétaire du compartiment appliqué pour Propriété d'objets, tenez compte de ce qui suit :
  >
  > - ACLs sont désactivés et n'affectent plus les autorisations. Vous ne pouvez pas mettre à jour la liste ACL de votre compartiment pour accorder l'accès au groupe de livraison des journaux S3. À la place, pour accorder l'accès au principal du service de journalisation, vous devez mettre à jour la politique de compartiment pour le compartiment de destination.
  > - Vous ne pouvez pas inclure d'octrois de destination dans votre configuration `PutBucketLogging`.

- La politique de compartiment du compartiment de destination permet d'accéder aux journaux : vérifiez la politique de compartiment du compartiment de destination. Recherchez dans la politique du compartiment toutes les déclarations contenant `"Effect": "Deny"`. Vérifiez ensuite que la déclaration `Deny` n'empêche pas l'écriture des journaux d'accès dans le compartiment.
- Le verrouillage d'objet S3 n'est pas activé sur le compartiment de destination : vérifiez si le verrouillage d'objet est activé dans le compartiment de destination. Le verrouillage des objets bloque la livraison des journaux d'accès au serveur. Vous devez choisir un compartiment de destination sur lequel le verrouillage d'objet n'est pas activé.
- Les clés gérées par Amazon S3 (SSE-S3) sont sélectionnées si le chiffrement par défaut est activé sur le compartiment de destination : vous pouvez utiliser le chiffrement de compartiment par défaut sur le compartiment de destination uniquement si vous utilisez le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3). Le chiffrement côté serveur par défaut avec des

clés AWS Key Management Service (AWS KMS) (SSE-KMS) n'est pas pris en charge pour les compartiments de destination de journalisation des accès au serveur. Pour plus d'informations sur l'activation du chiffrement par défaut, consultez Configuration du chiffrement par défaut.

- Le paiement par le demandeur n'est pas activé dans le compartiment de destination : le paiement par le demandeur n'est pas pris en charge dans le compartiment de destination pour la journalisation des accès au serveur. Pour autoriser la livraison des journaux d'accès au serveur, désactivez l'option Paiement par le demandeur sur le compartiment de destination.
- Passez en revue vos politiques de contrôle des AWS Organizations services (SCPs) et vos politiques de contrôle des ressources (RCPs) : lorsque vous utilisez AWS Organizations, vérifiez les politiques de contrôle des services et les politiques de contrôle des ressources pour vous assurer que l'accès à Amazon S3 est autorisé. Ces politiques spécifient les autorisations maximales pour les principaux et les ressources des comptes concernés. Recherchez dans les politiques toutes les instructions qui contiennent `"Effect": "Deny"` et vérifiez que les instructions `Deny` n'empêchent pas l'écriture des journaux d'accès dans le compartiment. Pour plus d'informations, consultez Politiques d'autorisation dans AWS Organizations dans le Guide de l'utilisateur AWS Organizations .
- Prévoyez un certain temps pour que les modifications récentes de la configuration de la journalisation prennent effet : l'activation de la journalisation des accès au serveur pour la première fois ou la modification du compartiment de destination pour les journaux nécessite du temps pour entrer pleinement en vigueur. Plus d'une heure peut être nécessaire pour que toutes les demandes soient correctement journalisées et livrées.

  Pour vérifier les échecs de livraison des journaux, activez les métriques de demande sur Amazon CloudWatch. Si les journaux ne sont pas livrés au bout de quelques heures, recherchez la métrique `4xxErrors`, qui peut indiquer des échecs de livraison des journaux. Pour plus d'informations sur l'activation des métriques de demande, consultez the section called "Création d'une configuration de métriques pour tous les objets".

Surveillance des métriques avec Amazon CloudWatch

CloudWatch Les métriques Amazon pour Amazon S3 peuvent vous aider à comprendre et à améliorer les performances des applications qui utilisent Amazon S3. Il existe plusieurs méthodes que vous pouvez utiliser CloudWatch avec Amazon S3.

Métriques du stockage quotidien pour les compartiments

Surveillez le stockage par compartiments à l'aide CloudWatch de ce qui collecte et traite les données de stockage d'Amazon S3 en indicateurs quotidiens lisibles. Ces métriques de stockage pour Amazon S3 sont fournis une fois par jour à tous les clients sans coût supplémentaire.

Métriques des demandes

Surveillez les demandes Amazon S3 pour identifier rapidement les problèmes opérationnels et agir en conséquences. Les métriques sont disponibles à des intervalles d'une minute après une latence de traitement. Ces CloudWatch statistiques sont facturées au même tarif que les statistiques CloudWatch personnalisées d'Amazon. Pour plus d'informations sur CloudWatch les tarifs, consultez CloudWatch les tarifs Amazon. Pour en savoir plus sur la façon d'obtenir ces métriques, consultez CloudWatch configurations de métriques.

Lorsqu'elles sont activées, les métriques de demandes sont indiquées pour toutes les opérations d'objets. Par défaut, ces métriques d'une minute sont disponibles au niveau du compartiment Amazon S3. Vous pouvez également définir un filtre pour les métriques à l'aide d'un préfixe partagé, d'une balise d'objet ou d'un point d'accès.

- Point d'accès – Les points d'accès sont nommés points de terminaison réseau qui sont associés à des compartiments et simplifient la gestion de l'accès aux données à grande échelle pour les jeux de données partagés dans S3. Avec le filtre de point d'accès, vous pouvez obtenir des informations sur l'utilisation de votre point d'accès. Pour plus d'informations sur les points d'accès, consultez Surveillance et journalisation des points d'accès.
- Préfixe – Même si le modèle de données Amazon S3 est une structure plane, vous pouvez induire une hiérarchie à l'aide d'un préfixe. Un préfixe est similaire à un nom de répertoire qui vous permet de regrouper des objets similaires dans un compartiment. La console S3 prend en charge ces préfixes avec le concept de dossiers. Si vous filtrez par préfixe, les objets ayant le même préfixe seront inclus dans la configuration des métriques. Pour en savoir plus sur les préfixes, consultez Organisation des objets à l'aide de préfixes.
- Balises – Vous pouvez ajouter des balises, à savoir des paires de noms clés-valeurs, aux objets. Les balises vous permettent de trouver et de classer facilement les objets. Vous pouvez également utiliser des balises comme filtre pour les configurations de métriques de sorte que seuls les objets avec ces balises soient inclus dans la configuration des métriques. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.

Pour faire correspondre ces métriques à des applications commerciales spécifiques, à des flux de travail ou à des organisation internes spécifiques, vous pouvez filtrer sur un préfixe partagé, une balise d'objet ou un point d'accès.

Métriques de réplication

Surveillez le nombre total d'opérations d'API S3 en attente de réplication, la taille totale des objets en attente de réplication et la durée maximale de réplication vers la Région AWS de destination, ainsi que le nombre total d'opérations pour lesquelles la réplication a échoué. Les règles de réplication sur lesquelles des métriques de réplication S3 ou Contrôle du temps de réplication S3 (S3 RTC) sont activées publient des métriques de réplication.

Pour plus d'informations, consultez Surveillance de la réplication avec des métriques, des notifications d'événements et des statuts ou Satisfaction aux exigences de conformité à l'aide du contrôle du temps de réplication S3.

Métriques Amazon S3 Storage Lens

Vous pouvez publier les statistiques d'utilisation et d'activité de S3 Storage Lens sur Amazon CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatch tableaux de bord. Les métriques S3 Storage Lens sont disponibles dans l'espace de noms `AWS/S3/Storage-Lens`. L'option de CloudWatch publication est disponible pour les tableaux de bord S3 Storage Lens mis à niveau vers des métriques et des recommandations avancées. Vous pouvez activer l'option de CloudWatch publication pour une configuration de tableau de bord nouvelle ou existante dans S3 Storage Lens.

Pour de plus amples informations, veuillez consulter Surveillez les métriques de S3 Storage Lens dans CloudWatch.

Toutes les CloudWatch statistiques sont conservées pendant une période de 15 mois afin que vous puissiez accéder aux informations historiques et avoir une meilleure idée des performances de votre application ou service Web. Pour plus d'informations CloudWatch, consultez Qu'est-ce qu'Amazon CloudWatch ? dans le guide de CloudWatch l'utilisateur Amazon. Il se peut que vous ayez besoin de configurations supplémentaires pour vos CloudWatch alarmes, en fonction de vos cas d'utilisation. Par exemple, vous pouvez utiliser une expression mathématique métrique pour créer une alarme. Pour plus d'informations, consultez CloudWatch les sections Utiliser des métriques, Utiliser des métriques mathématiques, Utiliser des CloudWatch alarmes Amazon et Créer une CloudWatch alarme basée sur une expression mathématique métrique dans le Guide de CloudWatch l'utilisateur Amazon.

Livraison des CloudWatch indicateurs les plus efficaces

CloudWatch les indicateurs sont fournis dans la mesure du possible. La plupart des demandes relatives à un objet Amazon S3 comportant des métriques de demande aboutissent à l'envoi d'un point de données à CloudWatch.

L'exhaustivité et la ponctualité des métriques ne sont pas garanties. Le point de données d'une demande particulière doit être retourné avec un horodatage ultérieur au moment du traitement de la demande. Le point de données peut être retardé d'une minute avant d'être disponible CloudWatch, ou il se peut qu'il ne soit pas livré du tout. CloudWatch les métriques de demande vous donnent une idée de la nature du trafic par rapport à votre compartiment en temps quasi réel. L'objectif n'est pas de comptabiliser toutes les demandes.

En conséquence de la nature du « meilleur effort » de cette fonction, les rapports disponibles sur le Tableau de bord Gestion de la facturation et des coûts peuvent inclure une ou plusieurs demandes d'accès qui ne figurent pas dans les métriques du compartiment.

Pour plus d'informations, consultez les rubriques suivantes.

Rubriques

- Métriques et dimensions
- Accès aux CloudWatch métriques
- CloudWatch configurations de métriques

Métriques et dimensions

Les métriques et dimensions de stockage qu'Amazon S3 envoie à Amazon CloudWatch sont répertoriées dans les tableaux suivants.

Livraison des CloudWatch indicateurs les plus efficaces

CloudWatch les indicateurs sont fournis dans la mesure du possible. La plupart des demandes relatives à un objet Amazon S3 comportant des métriques de demande aboutissent à l'envoi d'un point de données à CloudWatch.

L'exhaustivité et la ponctualité des métriques ne sont pas garanties. Le point de données d'une demande particulière doit être retourné avec un horodatage ultérieur au moment du traitement de la demande. Le point de données peut être retardé d'une minute avant d'être disponible CloudWatch, ou il se peut qu'il ne soit pas livré du tout. CloudWatch les métriques de demande vous donnent une idée de la nature du trafic par rapport à votre compartiment en temps quasi réel. L'objectif n'est pas de comptabiliser toutes les demandes.

En conséquence de la nature du « meilleur effort » de cette fonction, les rapports disponibles sur le Tableau de bord Gestion de la facturation et des coûts peuvent inclure une ou plusieurs demandes d'accès qui ne figurent pas dans les métriques du compartiment.

Rubriques

- Mesures de stockage quotidiennes d'Amazon S3 pour les compartiments CloudWatch
- Mesures de demande Amazon S3 dans CloudWatch
- Métriques de réplication S3 dans CloudWatch
- Métriques de S3 Storage Lens dans CloudWatch
- Métriques de demande Lambda d'un objet S3 dans CloudWatch
- Dimensions d'Amazon S3 dans CloudWatch
- Dimensions de réplication S3 dans CloudWatch
- Dimensions de l'objectif de rangement S3 en CloudWatch
- Dimensions de la demande Lambda de l'objet S3 dans CloudWatch
- Métriques d'utilisation Amazon S3

Mesures de stockage quotidiennes d'Amazon S3 pour les compartiments CloudWatch

L'espace de nom `AWS/S3` inclut les métriques quotidiennes de stockage suivantes pour les compartiments.

Métrique	Description
`BucketSizeBytes`	Quantité de données en octets stockée dans un compartiment dans les classes de stockage suivantes : • Stockage à redondance réduite (RRS) (`REDUCED_REDUNDANCY`) • S3 Express One Zone (`EXPRESS_ONEZONE`) • S3 Glacier Deep Archive (`DEEP_ARCHIVE`) • S3 Glacier Flexible Retrieval (`GLACIER`) • S3 Glacier Instant Retrieval (`GLACIER_IR`) • S3 Intelligent-Tiering (`INTELLIGENT_TIERING`) • S3 One Zone-Infrequent Access (`ONEZONE_IA`) • S3 Standard (`STANDARD`)

Métrique	Description
	• S3 Standard-Infrequent Access (`STANDARD_IA`) Cette valeur est calculée en effectuant la somme des tailles de tous les objets et métadonnées (tels que le nom des compartiments) au sein du compartiment (versions actuelles et anciennes des objets incluses), ce qui comprend également la taille de toutes les parties pour tous les chargements partitionnés incomplets dans le compartiment. **Note** La classe de stockage S3 Express One Zone n'est disponible que pour les compartiments de répertoires. Filtres de type de stockage valides (voir la dimension `StorageType`) : • Stockage à redondance réduite (RRS) : `ReducedRedundancyStorage` • S3 Express One Zone : `ExpressOneZoneStorage` • S3 Glacier Deep Archive : `DeepArchiveObjectOverhead`, `DeepArchiveS3ObjectOverhead`, `DeepArchiveStagingStorage`, `DeepArchiveStorage` • S3 Glacier Flexible Retrieval : `GlacierObjectOverhead`, `GlacierS3ObjectOverhead`, `GlacierStagingStorage`, `GlacierStorage` • S3 Glacier Instant Retrieval : `GlacierInstantRetrievalStorage`, `GlacierIRSizeOverhead` • S3 Intelligent-Tiering : `IntelligentTieringAAStorage`, `IntelligentTieringAIAStorage`, `IntelligentTieringDAAStorage`, `IntelligentTieringFAStorage`, `IntelligentTieringIAStorage` • S3 One Zone-Infrequent Access : `OneZoneIASizeOverhead`, `OneZoneIAStorage` • S3 Standard : `StandardStorage`

Métrique	Description
	• S3 Standard-Infrequent Access : `StandardIAObjectOverhead` , `StandardIASizeOverhead` , `StandardIAStorage` Unités : octets Statistiques valides : Moyenne Pour plus d'informations sur les dimensions `StorageType` , consultez the section called "Dimensions d'Amazon S3 dans CloudWatch".
`NumberOfObjects`	Nombre total d'objets stockés dans un compartiment à usage général pour toutes les classes de stockage. Cette valeur est calculée en comptant tous les objets au sein du compartiment, ce qui inclut les versions actuelles et anciennes des objets, les marqueurs de suppressi on, ainsi que le nombre total de parties pour tous les chargements partitionnés incomplets vers le compartiment. Pour les compartiments de répertoires contenant des objets de classe de stockage S3 Express One Zone, cette valeur est calculée en comptant tous les objets figurant dans le compartiment, mais elle n'inclut pas les chargements incomplets effectués dans le compartiment. Filtres de type de stockage valides : `AllStorageTypes` (voir la dimension `StorageType`) Unités : nombre Statistiques valides : Moyenne

Mesures de demande Amazon S3 dans CloudWatch

L'espace de nom `AWS/S3` inclut les métriques de demandes suivantes. Ces métriques incluent les demandes non facturables (dans le cas des demandes `GET` de l'opération `CopyObject` et du processus de réplication).

> **Note**
>
> Les métriques de requêtes Amazon S3 entrées CloudWatch ne sont pas prises en charge pour les compartiments d'annuaire.

Métrique	Description
`AllRequests`	Nombre total de demandes HTTP à destination d'un compartiment Amazon S3, quel que soit leur type. Si vous utilisez une configuration de métriques avec un filtre, cette métrique retourne uniquement les requêtes HTTP qui correspondent aux exigences du filtre. Unités : nombre Statistiques valides : somme
`GetRequests`	Nombre de requêtes HTTP `GET` exécutées pour des objets dans un compartiment Amazon S3. Cela n'inclut pas les opérations de liste. Cette métrique est incrémentée pour la source de chaque demande `CopyObject` . Unités : nombre Statistiques valides : somme **Note** Les demandes paginées axées sur les listes, telles que ListMultipartUploads, ListParts, ListObjectVersions et autres, ne sont pas incluses dans cette métrique.
`PutRequests`	Nombre de requêtes HTTP `PUT` exécutées pour des objets dans un compartiment Amazon S3. Cette métrique est incrémentée pour la destination de chaque demande `CopyObject` . Unités : nombre

Métrique	Description
	Statistiques valides : somme
`DeleteRequests`	Nombre de requêtes HTTP `DELETE` exécutées pour des objets dans un compartiment Amazon S3. Cette métrique inclut également les demandes DeleteObjects. Cette métrique indique le nombre de demandes effectuées, et non pas le nombre d'objets supprimés. Unités : nombre Statistiques valides : somme
`HeadRequests`	Nombre de requêtes HTTP `HEAD` effectuées pour un compartiment Amazon S3. Unités : nombre Statistiques valides : somme
`PostRequests`	Nombre de requêtes HTTP `POST` effectuées pour un compartiment Amazon S3. Unités : nombre Statistiques valides : somme **Note** Les demandes DeleteObjects et SelectObjectContent ne sont pas incluses dans cette métrique.
`SelectRequests`	Nombre de demandes SelectObjectContent Amazon S3 exécutées pour des objets dans un compartiment Amazon S3. Unités : nombre Statistiques valides : somme

Métrique	Description
`SelectBytesScanned`	Nombre d'octets de données analysées avec les demandes Amazon S3 SelectObjectContent dans un compartiment Amazon S3. Unités : octets Statistiques valides : Moyenne (octets par demande), Somme (octets par période), Exemple de comptage, Min, Max (identique à p100), tout percentile entre p0.0 et p99.9
`SelectBytesReturned`	Nombre d'octets de données renvoyés avec les demandes Amazon S3 SelectObjectContent dans un compartiment Amazon S3. Unités : octets Statistiques valides : Moyenne (octets par demande), Somme (octets par période), Exemple de comptage, Min, Max (identique à p100), tout percentile entre p0.0 et p99.9
`ListRequests`	Le nombre de requêtes HTTP qui répertorient le contenu d'un compartiment. Unités : nombre Statistiques valides : somme
`BytesDownloaded`	Nombre d'octets téléchargés pour les demandes adressées à un compartiment Amazon S3, pour lesquelles la réponse inclut un corps. Unités : octets Statistiques valides : Moyenne (octets par demande), Somme (octets par période), Exemple de comptage, Min, Max (identique à p100), tout percentile entre p0.0 et p99.9

Métrique	Description
`BytesUploaded`	Nombre d'octets téléchargés pour les requêtes adressées à un compartiment Amazon S3, pour lesquelles la réponse inclut un corps. Unités : octets Statistiques valides : Moyenne (octets par demande), Somme (octets par période), Exemple de comptage, Min, Max (identique à p100), tout percentile entre p0.0 et p99.9
`4xxErrors`	Nombre de demandes HTTP avec le code de statut d'erreur client 4xx adressées à un compartiment Amazon S3 avec une valeur de 0 ou 1. La statistique Average (Moyenne) indique le taux d'erreur et la statistiq ue Sum (Somme) indique le nombre de ce type d'erreur pendant chaque période. Unités : nombre Statistiques valides : Moyenne (rapports par demande), Somme (rapports par période), Min, Max, Exemple de comptage
`5xxErrors`	Nombre de demandes HTTP avec le code de statut d'erreur serveur 5xx adressées à un compartiment Amazon S3 avec une valeur de 0 ou 1. La statistique Average (Moyenne) indique le taux d'erreur et la statistiq ue Sum (Somme) indique le nombre de ce type d'erreur pendant chaque période. Unités : nombre Statistiques valides : Moyenne (rapports par demande), Somme (rapports par période), Min, Max, Exemple de comptage

Métrique	Description
`FirstByteLatency`	Temps par demande entre la réception de la demande complète par un compartiment Amazon S3 et le début du retour de la réponse. Unités : millisecondes Statistiques valides : Average (Moyenne), Sum (Somme), Min, Max (identique à p100), Sample Count (Nombre d'exemples), tout centile entre p0.0 et p100
`TotalRequestLatency`	Temps par demande écoulé entre la réception du premier octet et l'envoi du dernier octet à un compartiment Amazon S3. Cette métrique inclut le temps mis pour recevoir le corps de la requête et envoyer le corps de la réponse, qui n'est pas inclus dans `FirstByteLatency` . Unités : millisecondes Statistiques valides : Average (Moyenne), Sum (Somme), Min, Max (identique à p100), Sample Count (Nombre d'exemples), tout centile entre p0.0 et p100

Métriques de réplication S3 dans CloudWatch

Vous pouvez surveiller l'avancement de la réplication avec les métriques de réplication S3 en suivant les octets en attente, les opérations en attente et la latence de réplication. Pour plus d'informations, consultez Surveillance de l'avancement des métriques de réplication.

> **Note**
>
> Vous pouvez activer les alarmes pour vos métriques de réplication dans Amazon CloudWatch. Lorsque vous configurez des alarmes pour vos métriques de réplication, définissez le champ Missing data treatment (Traitement des données manquantes) sur Treat missing data as ignore (maintain the alarm state) (Ignorer les données manquantes [conserver l'état d'alarme]).

Métrique	Description
`ReplicationLatency`	Nombre maximal de secondes pendant lequel la destination de réplication se Région AWS trouve derrière la source Région AWS pour une règle de réplication donnée. Unités : secondes Statistiques valides : Max
`BytesPendingReplication`	Nombre total d'octets d'objets en attente de réplication pour une règle de réplication donnée. Unités : octets Statistiques valides : Max
`OperationsPendingReplication`	Nombre d'opérations en attente de réplication pour une règle de réplication donnée. Unités : nombre Statistiques valides : Max
`OperationsFailedReplication`	Nombre d'opérations pour lesquelles la réplication a échoué pour une règle de réplication donnée. Unités : nombre Statistiques valides : somme (nombre total d'opérations ayant échoué), moyenne (taux d'échec), nombre d'échantillons (nombre total d'opérations de réplication)

Métriques de S3 Storage Lens dans CloudWatch

Vous pouvez publier les statistiques d'utilisation et d'activité de S3 Storage Lens sur Amazon CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatchtableaux de bord. Les métriques S3 Storage Lens sont publiées dans l'espace de `AWS/S3/Storage-Lens` noms dans CloudWatch. L'option de CloudWatch publication est disponible

pour les tableaux de bord S3 Storage Lens qui ont été mis à niveau vers des métriques et des recommandations avancées.

Pour obtenir la liste des métriques de S3 Storage Lens publiées sur CloudWatch, consultezGlossaire des métriques Amazon S3 Storage Lens. Pour obtenir la liste complète des dimensions, consultez Dimensions.

Métriques de demande Lambda d'un objet S3 dans CloudWatch

S3 Object Lambda inclut les métriques de demande suivantes.

Métrique	Description
`AllRequests`	Nombre total de demandes HTTP exécutées sur un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda. Unités : nombre Statistiques valides : somme
`GetRequests`	Nombre de demandes HTTP `GET` exécutées pour des objets à l'aide d'un point d'accès Object Lambda. Cette métrique n'inclut pas les opérations de liste. Unités : nombre Statistiques valides : somme
`BytesUploaded`	Nombre d'octets chargés dans un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda, où la demande inclut un corps. Unités : octets Statistiques valides : Moyenne (octets par demande), Somme (octets par période), Exemple de comptage, Min, Max (identique à p100), tout percentile entre p0.0 et p99.9
`PostRequests`	Nombre de demandes HTTP `POST` exécutées sur un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda. Unités : nombre

Métrique	Description
	Statistiques valides : somme
`PutRequests`	Nombre de demandes HTTP `PUT` exécutées pour des objets dans un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda. Unités : nombre Statistiques valides : somme
`DeleteRequests`	Nombre de demandes HTTP `DELETE` exécutées pour des objets dans un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda. Cette métrique inclut les demandes DeleteObjects. Cette métrique indique le nombre de demandes effectuées, et non pas le nombre d'objets supprimés. Unités : nombre Statistiques valides : somme
`BytesDownloaded`	Nombre d'octets téléchargés pour les demandes adressées à un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda, pour lesquelles la réponse inclut un corps. Unités : octets Statistiques valides : Moyenne (octets par demande), Somme (octets par période), Exemple de comptage, Min, Max (identique à p100), tout percentile entre p0.0 et p99.9

Métrique	Description
`FirstByteLatency`	Temps par demande entre la réception de la demande complète par un compartiment Amazon S3 via un point d'accès Object Lambda et le début du renvoi de la réponse. Cette métrique dépend du temps d'exécution de la fonction AWS Lambda pour transformer l'objet avant que la fonction ne renvoie les octets au point d'accès Object Lambda. Unités : millisecondes Statistiques valides : Average (Moyenne), Sum (Somme), Min, Max (identique à p100), Sample Count (Nombre d'exemples), tout centile entre p0.0 et p100
`TotalRequestLatency`	Temps par demande écoulé entre la réception du premier octet et l'envoi du dernier octet à un point d'accès Object Lambda. Cette métrique inclut le temps mis pour recevoir le corps de la demande et envoyer le corps de la réponse, qui n'est pas inclus dans `FirstByteLatency` . Unités : millisecondes Statistiques valides : Average (Moyenne), Sum (Somme), Min, Max (identique à p100), Sample Count (Nombre d'exemples), tout centile entre p0.0 et p100
`HeadRequests`	Nombre de demandes HTTP `HEAD` exécutées sur un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda. Unités : nombre Statistiques valides : somme
`ListRequests`	Le nombre de requêtes HTTP `GET` qui répertorient le contenu d'un compartiment Amazon S3. Cette métrique inclut les opérations `ListObjects` et `ListObjectsV2` . Unités : nombre Statistiques valides : somme

Métrique	Description
`4xxErrors`	Nombre de demandes HTTP avec le code de statut d'erreur de serveur 4xx adressées à un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda avec la valeur 0 ou 1. La statistique Average (Moyenne) indique le taux d'erreur et la statistique Sum (Somme) indique le nombre de ce type d'erreur pendant chaque période. Unités : nombre Statistiques valides : Moyenne (rapports par demande), Somme (rapports par période), Min, Max, Exemple de comptage
`5xxErrors`	Nombre de demandes HTTP avec le code de statut d'erreur de serveur 5xx adressées à un compartiment Amazon S3 à l'aide d'un point d'accès Object Lambda avec une valeur de 0 ou 1. La statistique Average (Moyenne) indique le taux d'erreur et la statistique Sum (Somme) indique le nombre de ce type d'erreur pendant chaque période. Unités : nombre Statistiques valides : Moyenne (rapports par demande), Somme (rapports par période), Min, Max, Exemple de comptage
`ProxiedRequests`	Nombre de demandes HTTP adressées à un point d'accès Object Lambda qui renvoient la réponse d'API Amazon S3 standard. (Aucune fonction Lambda n'est configurée pour ces demandes.) Unités : nombre Statistiques valides : somme
`InvokedLambda`	Nombre de requêtes HTTP adressées à un objet S3 pour lesquelles une fonction Lambda a été invoquée. Unités : nombre Statistiques valides : somme

Métrique	Description
`LambdaResponseRequests`	Nombre de requêtes `WriteGetObjectResponse` effectuées par la fonction Lambda. Cette métrique s'applique uniquement aux requêtes `GetObject` .
`LambdaResponse4xx`	Nombre d'erreurs de client HTTP 4xx qui se produisent lors d'un appel à `WriteGetObjectResponse` à partir d'une fonction Lambda. Cette métrique fournit les mêmes informations que `4xxErrors` , mais uniquement pour les appels à `WriteGetObjectResponse` .
`LambdaResponse5xx`	Nombre d'erreurs de serveur HTTP 5xx qui se produisent lors d'un appel à `WriteGetObjectResponse` à partir d'une fonction Lambda. Cette métrique fournit les mêmes informations que `5xxErrors` , mais uniquement pour les appels à `WriteGetObjectResponse` .

Dimensions d'Amazon S3 dans CloudWatch

Les dimensions suivantes sont utilisées pour filtrer les métriques Amazon S3.

Dimension	Description
`BucketName`	Cette dimension filtre les données que vous demandez dans le compartiment identifié uniquement.
`StorageType`	Cette dimension filtre les données que vous avez enregistrées dans un compartiment en fonction des types de stockage : • `DeepArchiveObjectOverhead` – Pour chaque objet archivé, S3 Glacier ajoute 32 Ko de stockage pour l'index et les métadonnées associées. Ces données supplémentaires sont nécessaires pour identifier et restaurer l'objet. Le tarif S3 Glacier Deep Archive vous est facturé pour ce stockage supplémentaire. • `DeepArchiveS3ObjectOverhead` – Pour chaque objet archivé dans S3 Glacier Deep Archive, Simple Storage Service (Amazon S3) utilise 8 Ko de stockage pour le nom de

Dimension	Description
	l'objet et d'autres métadonnées. Le tarif S3 Standard vous est facturé pour ce stockage supplémentaire. • `DeepArchiveStagingStorage` – Nombre d'octets utilisés pour les parties des objets d'un chargement partition né avant la fin de l'exécution de la demande `CompleteMultipartUpload` sur ces objets dans la classe de stockage S3 Glacier Deep Archive. • `DeepArchiveStorage` – Nombre d'octets utilisés pour les objets dans la classe de stockage S3 Glacier Deep Archive. • `ExpressOneZoneStorage` : nombre d'octets utilisés pour les objets dans la classe de stockage S3 Express One Zone. • `GlacierInstantRetrievalStorage` – Nombre d'octets utilisés pour les objets dans la classe de stockage S3 Glacier Instant Retrieval. • `GlacierIRSizeOverhead` – Nombre d'octets utilisés pour les objets de taille inférieure à 128 Ko dans la classe de stockage S3 Glacier Instant Retrieval. • `GlacierObjectOverhead` – Pour chaque objet archivé, S3 Glacier ajoute 32 Ko de stockage pour l'index et les métadonnées associées. Ces données supplémentaires sont nécessaires pour identifier et restaurer l'objet. Le tarif S3 Glacier Flexible Retrieval vous est facturé pour ce stockage supplémentaire. • `GlacierS3ObjectOverhead` – Pour chaque objet archivé dans S3 Glacier Flexible Retrieval, Simple Storage Service (Amazon S3) utilise 8 Ko de stockage pour le nom de l'objet et d'autres métadonnées. Le tarif S3 Standard vous est facturé pour ce stockage supplémentaire. • `GlacierStagingStorage` – Nombre d'octets utilisés pour les parties des objets d'un chargement partitionné avant la fin de l'exécution de la demande `CompleteMultipartUpload` sur ces objets dans la classe de stockage S3 Glacier Flexible Retrieval.

Dimension	Description
	• `GlacierStorage` – Nombre d'octets utilisés pour les objets dans la classe de stockage S3 Glacier Flexible Retrieval. • `IntAAObjectOverhead` – Pour chaque objet de la classe de stockage `INTELLIGENT_TIERING` au niveau d'accès Archive, S3 Glacier ajoute 32 Ko de stockage pour l'index et les métadonnées associées. Ces données supplémentaires sont nécessaires pour identifier et restaurer l'objet. Le tarif S3 Glacier Flexible Retrieval vous est facturé pour ce stockage supplémentaire. • `IntAAS3ObjectOverhead` – Pour chaque objet de la classe de stockage `INTELLIGENT_TIERING` au niveau d'accès Archive, Amazon S3 utilise 8 Ko de stockage pour le nom de l'objet et les autres métadonnées. Le tarif S3 Standard vous est facturé pour ce stockage supplémentaire. • `IntDAAObjectOverhead` – Pour chaque objet de la classe de stockage `INTELLIGENT_TIERING` au niveau d'accès Deep Archive, S3 Glacier ajoute 32 Ko de stockage pour l'index et les métadonnées associées. Ces données supplémentaires sont nécessaires pour identifier et restaurer l'objet. Le tarif S3 Glacier Deep Archive vous est facturé pour ce stockage supplémentaire. • `IntDAAS3ObjectOverhead` – Pour chaque objet de la classe de stockage `INTELLIGENT_TIERING` au niveau d'accès Deep Archive, Amazon S3 ajoute 8 Ko de stockage pour l'index et les métadonnées associées. Ces données supplémentaires sont nécessaires pour identifier et restaurer l'objet. Le tarif S3 Standard vous est facturé pour ce stockage supplémentaire. • `IntelligentTieringAAStorage` – Nombre d'octets utilisés pour les objets du niveau d'accès Archive de la classe de stockage `INTELLIGENT_TIERING` .

Dimension	Description
	• `IntelligentTieringAIAStorage` – Nombre d'octets utilisés pour les objets du niveau d'accès Archive Instant de la classe de stockage `INTELLIGENT_TIERING` . • `IntelligentTieringDAAStorage` – Nombre d'octets utilisés pour les objets du niveau d'accès Deep Archive de la classe de stockage `INTELLIGENT_TIERING` . • `IntelligentTieringFAStorage` – Nombre d'octets utilisés pour les objets du niveau Accès fréquent de la classe de stockage `INTELLIGENT_TIERING` . • `IntelligentTieringIAStorage` – Nombre d'octets utilisés pour les objets du niveau Accès peu fréquent de la classe de stockage `INTELLIGENT_TIERING` . • `OneZoneIASizeOverhead` – Nombre d'octets utilisés pour les objets d'une taille inférieure à 128 Ko dans la classe de stockage `ONEZONE_IA` . • `OneZoneIAStorage` – Nombre d'octets utilisés pour les objets dans la classe de stockage S3 One Zone-Infrequent Access (`ONEZONE_IA`). • `ReducedRedundancyStorage` – Nombre d'octets utilisés pour les objets dans la classe de stockage à redondance réduite (RRS). • `StandardIASizeOverhead` – Nombre d'octets utilisés pour les objets d'une taille inférieure à 128 Ko dans la classe de stockage `STANDARD_IA` . • `StandardIAStorage` – Nombre d'octets utilisés pour les objets de la classe de stockage S3 Standard-Infrequent Access (`STANDARD_IA`). • `StandardStorage` – Nombre d'octets utilisés pour les objets dans la classe de stockage `STANDARD`.

Dimension	Description
`FilterId`	Cette dimension filtre les configurations de métriques que vous spécifiez pour les métriques de demande sur un compartiment. Lorsque vous créez une configuration de métriques, vous spécifiez un ID de filtre (par exemple, un préfixe, une balise ou un point d'accès). Pour plus d'informations, consultez Création d'une configuration de métriques.

Dimensions de réplication S3 dans CloudWatch

Les dimensions suivantes sont utilisées pour filtrer les métriques de réplication S3.

Dimension	Description
`SourceBucket`	Nom du compartiment à partir duquel les objects sont répliqués.
`DestinationBucket`	Nom du compartiment vers lequel les objets sont répliqués.
`RuleId`	Identifiant unique de la règle qui a déclenché la mise à jour de cette métrique de réplication.

Dimensions de l'objectif de rangement S3 en CloudWatch

Pour obtenir la liste des dimensions utilisées pour filtrer les métriques de S3 Storage Lens CloudWatch, consultezDimensions.

Dimensions de la demande Lambda de l'objet S3 dans CloudWatch

Les dimensions suivantes sont utilisées pour filtrer les données à partir d'un point d'accès Object Lambda.

Dimension	Description
`AccessPointName`	Le nom du point d'accès pour lequel les demandes sont effectuées.
`DataSourceARN`	La source à partir de laquelle le point d'accès Object Lambda récupère les données. Si la demande invoque une fonction Lambda, cela fait

Dimension	Description
	référence à l'Amazon Resource Name (ARN) Lambda. Sinon, cela fait référence à l'ARN du point d'accès.

Métriques d'utilisation Amazon S3

Vous pouvez utiliser les statistiques CloudWatch d'utilisation pour obtenir une visibilité sur l'utilisation des ressources par votre compte. Utilisez ces indicateurs pour visualiser l'utilisation actuelle de vos services sur CloudWatch des graphiques et des tableaux de bord.

Les métriques d'utilisation d'Amazon S3 correspondent aux quotas AWS de service. Vous pouvez configurer des alarmes qui vous alertent lorsque votre utilisation approche d'un quota de service. Pour plus d'informations sur CloudWatch l'intégration avec les quotas de service, consultez les statistiques AWS d'utilisation dans le guide de CloudWatch l'utilisateur Amazon.

Amazon S3 publie les métriques suivantes dans l'espace de noms `AWS/Usage`.

Métrique	Description
`ResourceCount`	Nombre des ressources spécifiées exécutées dans votre compte. Les ressources sont définies par les dimensions associées à la métrique.

Les dimensions suivantes permettent d'affiner les métriques d'utilisation publiées par Amazon S3.

Dimension	Description
`Service`	Nom du AWS service contenant la ressource. Pour les métriques d'utilisation d'Amazon S3, la valeur de cette dimension est `S3`.
`Type`	Type d'entité faisant l'objet d'un rapport. Actuellement, la seule valeur valide pour les métriques d'utilisation d'Amazon S3 est `Resource`.
`Resource`	Type de ressource en cours d'exécution. Actuellement, la seule valeur valide pour les métriques d'utilisation d'Amazon

Dimension	Description
	S3 est `GeneralPurposeBuckets` , qui renvoie le nombre de compartiments à usage général dans un Compte AWS. Les compartiments à usage général autorisent les objets stockés dans toutes les classes de stockage, à l'exception de S3 Express One Zone.

Accès aux CloudWatch métriques

Vous pouvez utiliser les procédures suivantes pour afficher les métriques de stockage d'Amazon S3. Pour obtenir les métriques Amazon S3 concernées, vous devez définir un horodatage de début et de fin. Pour les métriques portant sur une période de 24 heures, définissez la période sur 86 400 secondes, c'est-à-dire le nombre de secondes dans une journée. Vous devez également définir les dimensions `BucketName` et `StorageType`.

À l'aide du AWS CLI

Par exemple, si vous souhaitez utiliser le AWS CLI pour obtenir la moyenne de la taille d'un compartiment spécifique en octets, vous pouvez utiliser la commande suivante :

```
aws cloudwatch get-metric-statistics --metric-name BucketSizeBytes --namespace AWS/S3
 --start-time 2016-10-19T00:00:00Z --end-time 2016-10-20T00:00:00Z --statistics Average
 --unit Bytes --region us-west-2 --dimensions Name=BucketName,Value=amzn-s3-demo-bucket
 Name=StorageType,Value=StandardStorage --period 86400 --output json
```

Cet exemple produit le résultat suivant :

```
{
    "Datapoints": [
        {
            "Timestamp": "2016-10-19T00:00:00Z",
            "Average": 1025328.0,
            "Unit": "Bytes"
        }
    ],
    "Label": "BucketSizeBytes"
}
```

Utilisation de la console S3

Pour consulter les statistiques à l'aide de la CloudWatch console Amazon

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation de gauche, choisissez Métriques.
3. Choisissez l'espace de nom S3.
4. (Facultatif) Pour afficher une métrique, saisissez son nom dans la zone de recherche.
5. (Facultatif) Pour filtrer par StorageTypedimension, entrez le nom de la classe de stockage dans le champ de recherche.

Pour consulter la liste des mesures valides enregistrées pour votre compte à Compte AWS l'aide du AWS CLI

- À partir d'une invite de commande, utilisez la commande suivante :

```
aws cloudwatch list-metrics --namespace "AWS/S3"
```

Pour plus d'informations sur les autorisations requises pour accéder aux CloudWatch tableaux de bord, consultez les autorisations des tableaux CloudWatch de bord Amazon dans le guide de l' CloudWatch utilisateur Amazon.

CloudWatch configurations de métriques

Avec Amazon CloudWatch Request Metrics pour Amazon S3, vous pouvez recevoir des CloudWatch métriques d'une minute, configurer des CloudWatch alarmes et accéder à CloudWatch des tableaux de bord pour visualiser les near-real-time opérations et les performances de votre stockage Amazon S3. Pour les applications qui dépendent d'un stockage dans le Cloud, ces métriques vous permettent d'identifier rapidement les problèmes opérationnels et d'agir en conséquence. Lorsqu'elles sont activées, ces métriques d'1 minute sont disponibles par défaut au niveau du compartiment Amazon S3.

Si vous souhaitez obtenir les métriques de CloudWatch demande pour les objets d'un bucket, vous devez créer une configuration de métriques pour le bucket. Pour de plus amples informations, veuillez consulter Création d'une configuration de CloudWatch métriques pour tous les objets de votre compartiment.

Vous pouvez également utiliser un préfixe partagé, des balises d'objet ou un point d'accès pour définir un filtre pour les métriques collectées. Cette méthode de définition de filtre vous permet de faire correspondre les filtres des métriques à des applications métier, des flux de travail ou des organisations internes spécifiques. Pour de plus amples informations, veuillez consulter Création d'une configuration de métriques qui filtre par préfixe, balise d'objet ou point d'accès. Pour plus d'informations sur les métriques CloudWatch disponibles et sur les différences entre les métriques du stockage et les métriques des demandes, consultez Surveillance des métriques avec Amazon CloudWatch.

Gardez ces conseils à l'esprit lorsque vous utilisez les configurations de métriques :

- Vous pouvez avoir 1 000 configurations de métriques maximum par compartiment.
- Vous pouvez utiliser des filtres pour choisir les objets d'un compartiment à inclure dans les configurations de métriques. Vous pouvez filtrer sur un préfixe partagé, une balise d'objet ou un point d'accès pour aligner les filtres des métriques sur des applications commerciales, des flux de travail ou des organisations internes spécifiques. Pour demander des métriques pour le compartiment entier, créez une configuration de métriques sans filtre.
- Les configurations de métriques ne sont nécessaires que pour activer les métriques de demandes. Les métriques quotidiennes de stockage au niveau des compartiments sont toujours activées et sont fournies sans frais supplémentaires. Actuellement, il n'est pas possible d'obtenir des métriques de stockage quotidiennes pour un sous-ensemble d'objets filtré.
- Chaque configuration de métriques active l'ensemble complet de métriques de demandes disponibles. Les métriques spécifiques à une opération (telles que `PostRequests`) ne sont indiquées que s'il existe des demandes de ce type pour votre compartiment ou votre filtre.
- Les métriques de demandes sont indiquées pour toutes les opérations au niveau des objets. Elles sont également signalées pour les opérations qui répertorient le contenu du compartiment, comme GET Bucket (List Objects), GET Bucket Object Versions et List Multipart Uploads. En revanche, elles ne sont pas signalées pour les autres opérations sur les compartiments.
- Les métriques de demandes prennent en charge le filtrage par préfixe, balise d'objet ou point d'accès, contrairement aux métriques de stockage.

Livraison des CloudWatch indicateurs les plus efficaces

CloudWatch les indicateurs sont fournis dans la mesure du possible. La plupart des demandes relatives à un objet Amazon S3 comportant des métriques de demande aboutissent à l'envoi d'un point de données à CloudWatch.

L'exhaustivité et la ponctualité des métriques ne sont pas garanties. Le point de données d'une demande particulière doit être retourné avec un horodatage ultérieur au moment du traitement de la demande. Le point de données peut être retardé d'une minute avant d'être disponible CloudWatch, ou il se peut qu'il ne soit pas livré du tout. CloudWatch les métriques de demande vous donnent une idée de la nature du trafic par rapport à votre compartiment en temps quasi réel. L'objectif n'est pas de comptabiliser toutes les demandes.

En conséquence de la nature du « meilleur effort » de cette fonction, les rapports disponibles sur le Tableau de bord Gestion de la facturation et des coûts peuvent inclure une ou plusieurs demandes d'accès qui ne figurent pas dans les métriques du compartiment.

Pour plus d'informations sur l'utilisation des CloudWatch métriques dans Amazon S3, consultez les rubriques suivantes.

Rubriques

- Création d'une configuration de CloudWatch métriques pour tous les objets de votre compartiment
- Création d'une configuration de métriques qui filtre par préfixe, balise d'objet ou point d'accès
- Suppression d'un filtre de métriques

Création d'une configuration de CloudWatch métriques pour tous les objets de votre compartiment

Lorsque vous configurez les métriques de demande, vous pouvez créer une configuration de CloudWatch métriques pour tous les objets de votre bucket, ou vous pouvez filtrer par préfixe, balise d'objet ou point d'accès. Les procédures décrites dans cette rubrique vous montrent comment créer une configuration pour tous les objets de votre compartiment. Pour créer une configuration qui filtre par balise, préfixe d'objet ou point d'accès, consultez Création d'une configuration de métriques qui filtre par préfixe, balise d'objet ou point d'accès.

Il existe trois types de CloudWatch métriques Amazon pour Amazon S3 : les métriques de stockage, les métriques de demande et les métriques de réplication. Les métriques du stockage sont fournies une fois par jour à tous les clients sans frais supplémentaires. Ces métriques de demande sont disponibles à des intervalles d'une minute après une latence pour le traitement. Les métriques relatives aux demandes sont facturées au CloudWatch tarif standard. Vous devez activer les métriques de demande en les configurant dans la console ou en utilisant l'API Amazon S3. Les métriques de réplication S3 fournissent des métriques détaillées pour les règles de réplication dans votre configuration de réplication. Grâce aux métriques de réplication, vous pouvez suivre la minute-

by-minute progression en suivant les octets en attente, les opérations en attente, les opérations dont la réplication a échoué et la latence de réplication.

Pour plus d'informations sur CloudWatch les métriques pour Amazon S3, consultezSurveillance des métriques avec Amazon CloudWatch.

Vous pouvez ajouter des configurations de métriques à un compartiment à l'aide de la console Amazon S3, de l' AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3.

Utiliser la console S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant les objets pour lesquels vous souhaitez demander des métriques.
4. Sélectionnez l'onglet Métriques.
5. Sous Bucket metrics (Métriques de compartiment), choisissez View additional charts (Afficher des graphiques supplémentaires).
6. Choisissez l'onglet Request metrics (Métriques de demande).
7. Choisissez Create filter (Créer un filtre).
8. Dans la zone Filter name (Nom du filtre), saisissez un nom de filtre.

   Les noms peuvent contenir uniquement des lettres, des chiffres, des points, des tirets et des traits de soulignement. Nous vous recommandons d'utiliser le nom `EntireBucket` pour un filtre qui s'applique à tous les objets.
9. Sous Portée de filtre, choisissez Ce filtre s'applique à tous les objets du compartiment.

   Vous pouvez également définir un filtre pour collecter les métriques relatives à un sous-ensemble d'objets stockés dans le compartiment et générer le rapport correspondant. Pour plus d'informations, consultez Création d'une configuration de métriques qui filtre par préfixe, balise d'objet ou point d'accès.
10. Sélectionnez Save Changes (Enregistrer les modifications).
11. Sous l'onglet Métriques de demande, sous Filtres, choisissez le filtre que vous venez de créer.

    Après environ 15 minutes, CloudWatch commence à suivre ces métriques de demande. Vous pouvez les afficher dans l'onglet Request metrics (Métriques de demande). Vous pouvez

consulter les graphiques des métriques sur Amazon S3 ou sur CloudWatch la console. Les métriques relatives aux demandes sont facturées au CloudWatch tarif standard. Pour plus d'informations, consultez les CloudWatch tarifs Amazon.

Utilisation de l'API REST

Vous pouvez également ajouter des configurations de métriques par programmation avec l'API REST Amazon S3. Pour en savoir plus sur l'ajout et l'utilisation de configurations de métriques, consultez les rubriques suivantes dans la Référence d'API Amazon Simple Storage Service :

- Configuration de métriques PUT Bucket
- Configuration de métriques GET Bucket
- Configuration de métriques List Bucket
- Configuration de métriques DELETE Bucket

À l'aide du AWS CLI

1. Installez et configurez le AWS CLI. Pour obtenir des instructions, consultez Installation, mise à jour et désinstallation de l' AWS CLI dans le Guide de l'utilisateur de la AWS Command Line Interface .
2. Ouvrez un terminal.
3. Exécutez la commande suivante pour ajouter une configuration de métriques :

```
aws s3api put-bucket-metrics-configuration --endpoint https://s3.us-
west-2.amazonaws.com --bucket bucket-name --id metrics-config-id --metrics-
configuration '{"Id":"metrics-config-id"}'
```

Création d'une configuration de métriques qui filtre par préfixe, balise d'objet ou point d'accès

Il existe trois types de CloudWatch métriques Amazon pour Amazon S3 : les métriques de stockage, les métriques de demande et les métriques de réplication. Les métriques du stockage sont fournies une fois par jour à tous les clients sans frais supplémentaires. Ces métriques de demande sont disponibles à des intervalles d'une minute après une latence pour le traitement. Les métriques relatives aux demandes sont facturées au CloudWatch tarif standard. Vous devez activer les métriques de demande en les configurant dans la console ou en utilisant l'API Amazon S3. Les

métriques de réplication S3 fournissent des métriques détaillées pour les règles de réplication dans votre configuration de réplication. Grâce aux métriques de réplication, vous pouvez suivre la minute-by-minute progression en suivant les octets en attente, les opérations en attente, les opérations dont la réplication a échoué et la latence de réplication.

Pour plus d'informations sur CloudWatch les métriques pour Amazon S3, consultezSurveillance des métriques avec Amazon CloudWatch.

Lorsque vous configurez CloudWatch les métriques, vous pouvez créer un filtre pour tous les objets de votre bucket, ou vous pouvez filtrer la configuration en groupes d'objets connexes au sein d'un même bucket. Vous pouvez filtrer les objets d'un compartiment pour l'inclusion dans une configuration de métriques sur la base de l'un ou de plusieurs des types de filtre suivants :

- Préfixe de nom de clé d'objet – Même si le modèle de données Amazon S3 est une structure plane, vous pouvez induire une hiérarchie au moyen d'un préfixe. La console Amazon S3 prend en charge ces préfixes avec le concept de dossiers. Si vous filtrez par préfixe, les objets ayant le même préfixe seront inclus dans la configuration des métriques. Pour en savoir plus sur les préfixes, consultez Organisation des objets à l'aide de préfixes.
- Balise – Vous pouvez ajouter des balises, à savoir des paires de noms clés-valeurs, aux objets. Les balises vous permettent de trouver et de classer facilement les objets. Ces balises peuvent également être utilisées comme filtres pour les configurations de métriques. Pour en savoir plus sur les balises d'objet, consultez Catégorisation de vos objets à l'aide de balises.
- Point d'accès – Les points d'accès S3 sont nommés points de terminaison réseaux qui sont attachés à des compartiments et simplifient la gestion de l'accès aux données à l'échelle pour les jeux de données partagés dans S3. Lorsque vous créez un filtre de point d'accès, Amazon S3 inclut les demandes au point d'accès que vous indiquez dans la configuration des métriques. Pour plus d'informations, consultez Surveillance et journalisation des points d'accès.

> **Note**
>
> Lorsque vous créez une configuration de métriques qui filtre par point d'accès, vous devez utiliser Amazon Resource Name (ARN) du point d'accès, et non l'alias du point d'accès. Veillez à utiliser l'ARN pour le point d'accès lui-même, et non l'ARN pour un objet particulier. Pour plus d'informations sur le point d'accès ARNs, consultezUtilisation des points d'accès Amazon S3 pour des compartiments à usage général.

Si vous spécifiez un filtre, seules les demandes qui agissent sur des objets uniques peuvent correspondre au filtre et être incluses dans les métriques indiquées. Les demandes telles que DeleteObjects et `ListObjects` ne renvoient aucune métrique pour les configurations avec filtres.

Pour demander un filtrage plus complexe, choisissez deux ou plusieurs éléments. Seuls les objets possédant tous ces éléments sont inclus dans la configuration des métriques. Si vous ne définissez pas de filtres, tous les objets du compartiment sont inclus dans la configuration des métriques.

Utiliser la console S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, sélectionnez Buckets à usage général
3. Dans la liste des compartiments, choisissez le nom du compartiment contenant les objets pour lesquels vous souhaitez demander des métriques.
4. Choisissez l'onglet Métriques.
5. Sous Bucket metrics (Métriques de compartiment), choisissez View additional charts (Afficher des graphiques supplémentaires).
6. Choisissez l'onglet Request metrics (Métriques de demande).
7. Choisissez Create filter (Créer un filtre).
8. Dans la zone Filter name (Nom du filtre), saisissez un nom de filtre.

   Les noms peuvent contenir uniquement des lettres, des chiffres, des points, des tirets et des traits de soulignement.
9. Sous Portée du filtre, choisissez Limiter la portée de ce filtre à l'aide d'un préfixe, de balises d'objet et d'un point d'accès S3, ou d'une combinaison des trois.
10. Sous Type de filtre, choisissez au moins un type de filtre : Préfixe, Balises d'objet ou Point d'accès.
11. Pour définir un filtre de préfixe et limiter la porté du filtre à un seul chemin, saisissez un préfixe dans la zone Préfixe.
12. Pour définir un filtre de balises d'objet, sous Balises d'objet, choisissez Ajouter une balise, puis saisissez une balise Clé et Valeur.
13. Pour définir un filtre de point d'accès, dans le champ Point d'accès S3, saisissez l'ARN du point d'accès ou choisissez Parcourir S3 pour parvenir au point d'accès.

> **Important**
>
> Vous ne pouvez pas saisir l'alias d'un point d'accès. Vous devez saisir l'ARN du point d'accès lui-même, et non l'ARN d'un objet spécifique.

14. Sélectionnez Enregistrer les modifications.

    Amazon S3 crée un filtre qui utilise le préfixe, les balises ou le point d'accès que vous avez indiqués.

15. Sous l'onglet Métriques de demande, sous Filtres, choisissez le filtre que vous venez de créer.

    Vous avez maintenant créé un filtre qui limite la portée des métriques des demandes par préfixe, balises d'objet ou point d'accès. Environ 15 minutes après le CloudWatch début du suivi de ces métriques de demande, vous pouvez consulter les graphiques des métriques sur Amazon S3 et sur CloudWatch les consoles. Les métriques relatives aux demandes sont facturées au CloudWatch tarif standard. Pour plus d'informations, consultez les CloudWatch tarifs Amazon.

    Vous pouvez également configurer les métriques des demandes au niveau d'un compartiment. Pour plus d'informations, consultez Création d'une configuration de CloudWatch métriques pour tous les objets de votre compartiment.

À l'aide du AWS CLI

1. Installez et configurez le AWS CLI. Pour obtenir des instructions, consultez Installation, mise à jour et désinstallation de l' AWS CLI dans le Guide de l'utilisateur de la AWS Command Line Interface .
2. Ouvrez un terminal.
3. Pour ajouter une configuration de métriques, exécutez l'une des commandes suivantes :

   Example : pour filtrer par préfixe

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"Prefix":"prefix1"}} '
```

Example : pour filtrer par balises

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"Tag": {"Key": "string", "Value": "string"}} '
```

Example : pour filtrer par point d'accès

```
aws s3api put-bucket-metrics-configuration --bucket amzn-s3-demo-bucket --
id metrics-config-id --metrics-configuration '{"Id":"metrics-config-id", "Filter":
{"AccessPointArn":"arn:aws:s3:Region:account-id:accesspoint/access-point-name"}} '
```

Example : pour filtrer par préfixe, balises et point d'accès

```
aws s3api put-bucket-metrics-configuration --endpoint https://
s3.Region.amazonaws.com --bucket amzn-s3-demo-bucket --id metrics-config-id --
metrics-configuration '
{
    "Id": "metrics-config-id",
    "Filter": {
        "And": {
            "Prefix": "string",
            "Tags": [
                {
                    "Key": "string",
                    "Value": "string"
                }
            ],
            "AccessPointArn": "arn:aws:s3:Region:account-id:accesspoint/access-
point-name"
        }
    }
}'
```

Utilisation de l'API REST

Vous pouvez également ajouter des configurations de métriques par programmation avec l'API REST Amazon S3. Pour en savoir plus sur l'ajout et l'utilisation de configurations de métriques, consultez les rubriques suivantes dans la Référence d'API Amazon Simple Storage Service :

- Configuration de métriques PUT Bucket
- Configuration de métriques GET Bucket
- Configuration de métriques List Bucket
- Configuration de métriques DELETE Bucket

Suppression d'un filtre de métriques

Vous pouvez supprimer un filtre de statistiques de CloudWatch demande Amazon si vous n'en avez plus besoin. Lorsque vous supprimez un filtre, les métriques des demandes qui utilisent ce filtre spécifiquene vous sont plus facturées. Toutefois, vous continuerez à être facturé pour toute autre configuration de filtre existante.

Lorsque vous supprimez un filtre, vous ne pouvez plus l'utiliser pour les métriques des demandes. La suppression d'un filtre ne peut pas être annulée.

Pour plus d'informations sur la création d'un filtre de métriques des demandes, consultez les rubriques suivantes :

- Création d'une configuration de CloudWatch métriques pour tous les objets de votre compartiment
- Création d'une configuration de métriques qui filtre par préfixe, balise d'objet ou point d'accès

Utilisation de la console S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des buckets, choisissez le nom du bucket pour lequel vous souhaitez supprimer un filtre de métriques de demande.
4. Choisissez l'onglet Métriques.
5. Sous Bucket metrics (Métriques de compartiment), choisissez View additional charts (Afficher des graphiques supplémentaires).
6. Choisissez l'onglet Request metrics (Métriques de demande).
7. Choisissez Manage filters (Gérer les filtres).
8. Choisissez votre filtre.

> **Important**
>
> La suppression d'un filtre ne peut pas être annulée.

9. Sélectionnez Delete.

   Amazon S3 supprime votre filtre.

Utilisation de l'API REST

Vous pouvez également ajouter des configurations de métriques par programmation avec l'API REST Amazon S3. Pour en savoir plus sur l'ajout et l'utilisation de configurations de métriques, consultez les rubriques suivantes dans la Référence d'API Amazon Simple Storage Service :

- Configuration de métriques PUT Bucket
- Configuration de métriques GET Bucket
- Configuration de métriques List Bucket
- Configuration de métriques DELETE Bucket

Notifications d'événements Amazon S3

Vous pouvez utiliser la fonctionnalité Notifications d'événements Amazon S3 pour recevoir des notifications lorsque certains événements se produisent dans votre compartiment S3. Pour activer les notifications, ajoutez une configuration de notification qui identifie les événements que Amazon S3 doit publier. Assurez-vous que les destinations auxquelles Amazon S3 doit envoyer les notifications sont également identifiées. Vous stockez cette configuration dans la sous-ressource notification associée au compartiment. Pour plus d'informations, consultez Options de configuration des buckets à usage général. Amazon S3 fournit une API qui vous permet de gérer cette sous-ressource.

> **Important**
>
> Les notifications d'événement Amazon S3 sont conçues pour être délivrées au moins une fois. Les notifications d'événements parviennent généralement à destination en quelques secondes, mais cela peut aussi prendre une minute ou plus.

Présentation des notifications d'événements Amazon S3.

Actuellement, Amazon S3 peut publier des notifications pour les événements suivants :

- Événements créés par un nouvel objet
- Événements de suppression d'objets
- Événements de restauration d'objet
- Un événement de perte d'un objet Reduced Redundancy Storage (RRS)
- Événements de réplication
- Événements d'expiration du cycle de vie S3
- Événements de transition du cycle de vie S3
- Événements d'archivage automatique S3 Intelligent-Tiering
- Événements de balisage d'objets
- Événements PUT de liste ACL de l'objet

Pour obtenir des descriptions complètes de tous les types d'événement pris en charge, consultez Types d'événements pris en charge pour SQS, SNS et Lambda.

Amazon S3 peut envoyer des messages de notification d'événement vers les types de destination suivants : Vous devez spécifier l'Amazon Resource Name (ARN) de ces destinations dans la configuration des notifications.

- Rubriques Amazon Simple Notification Service (Amazon SNS)
- Files d'attente Amazon Simple Queue Service (Amazon SQS)
- AWS Lambda fonction
- Amazon EventBridge

Pour de plus amples informations, veuillez consulter Destinations d'événements prises en charge.

> **Note**
>
> Les files d'attente Amazon Simple Queue Service FIFO (premier entré, premier sorti) ne sont pas prises en charge en tant que destination des notifications d'événements Amazon S3. Pour envoyer une notification concernant un événement Amazon S3 à une file d'attente FIFO

Amazon SQS, vous pouvez utiliser Amazon. EventBridge Pour de plus amples informations, veuillez consulter Activation d'Amazon EventBridge.

Warning

Lorsque votre notification écrit dans le compartiment qui déclenche la notification, cela peut provoquer une boucle d'exécution. Par exemple, si le compartiment déclenche une fonction Lambda chaque fois qu'un objet est chargé et que la fonction charge un objet dans le compartiment, elle 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.

Pour plus d'informations et un exemple d'utilisation des notifications Amazon S3 avec AWS Lambda, consultez la section Utilisation AWS Lambda avec Amazon S3 dans le guide du AWS Lambda développeur.

Pour plus d'informations sur le nombre de configurations de notifications d'événements que vous pouvez créer par compartiment, consultez Quotas de service Amazon S3 dans la Référence générale d'AWS .

Pour plus d'informations sur les notifications d'événements, consultez les sections suivantes.

Rubriques

- Types de notification d'événements et destinations associées
- Utilisation d'Amazon SQS, Amazon SNS et Lambda
- En utilisant EventBridge

Types de notification d'événements et destinations associées

Amazon S3 prend en charge plusieurs types et destinations de notifications d'événements. Vous pouvez spécifier le type d'événement et la destination lors de la configuration de vos notifications. Une seule destination peut être spécifiée pour chaque notification d'événement. Les notifications d'événements Amazon S3 envoient une entrée d'événement pour chaque message de notification.

Rubriques

- Destinations d'événements prises en charge

- Types d'événements pris en charge pour SQS, SNS et Lambda
- Types d'événements pris en charge pour Amazon EventBridge
- Ordre des événements et doublons

Destinations d'événements prises en charge

Amazon S3 peut envoyer des messages de notification d'événement vers les types de destination suivants :

- Rubriques Amazon Simple Notification Service (Amazon SNS)
- Files d'attente Amazon Simple Queue Service (Amazon SQS)
- AWS Lambda
- Amazon EventBridge

Cependant, un seul type de destination peut être spécifié pour chaque notification d'événement.

> **Note**
>
> Vous devez autoriser Amazon S3 à publier des messages dans une rubrique Amazon SNS ou une file d'attente Amazon SQS. Vous devez également autoriser Amazon S3 à appeler une AWS Lambda fonction en votre nom. Pour obtenir des instructions sur la façon d'accorder ces autorisations, consultez Octroi d'autorisations pour la publication de messages de notification d'événement vers une destination.

Rubrique Amazon SNS

Amazon SNS est un service de messagerie de type Push flexible et totalement géré. Vous pouvez utiliser ce service pour envoyer des messages en mode Push vers des appareils mobiles ou des services distribués. Grâce à SNS, vous pouvez publier un message, puis le diffuser à une ou plusieurs reprises. Actuellement, SNS standard n'est autorisé qu'en tant que destination de notification d'événement S3, tandis que les rubriques FIFO SNS ne sont pas autorisées.

Amazon SNS coordonne et gère l'envoi et la diffusion de messages aux points de terminaison ou aux clients abonnés. Vous pouvez utiliser la console Amazon SNS pour créer la rubrique Amazon SNS qui recevra vos notifications.

Le sujet doit se trouver dans le même Région AWS que celui de votre compartiment Amazon S3. Pour obtenir des instructions sur comment créer une rubrique Amazon SNS, consultez Démarrer avec Amazon SNS dans le Manuel du développeur Amazon Simple Notification Service, ainsi que les Questions fréquentes (FAQ) sur Amazon SNS.

Pour pouvoir utiliser la rubrique Amazon SNS que vous avez créé en tant que destination d'une notification d'événements, vous devez disposer des éléments suivants :

- Amazon Resource Name (ARN) de la rubrique Amazon SNS
- Un abonnement à la rubrique Amazon SNS valide. Grâce à cela, les abonnés à la rubrique reçoivent une notification lorsqu'un message est publié sur votre rubrique Amazon SNS.

File d'attente Amazon SQS

Amazon SQS offre des files d'attente hébergées, évolutives et fiables dédiées au stockage des messages pendant leur circulation entre les ordinateurs. Amazon SQS vous permet de transmettre n'importe quel volume de données, sans nécessiter que d'autres services soient toujours disponibles. Vous pouvez utiliser la console Amazon SQS pour créer une file d'attente Amazon SQS qui recevra vos notifications.

La file d'attente Amazon SQS doit être Région AWS identique à celle de votre compartiment Amazon S3. Pour obtenir des instructions sur comment créer une file d'attente Amazon SQS, consultez les sections Qu'est-ce qu'Amazon Simple Queue Service et Mise en route avec Amazon SQS du Manuel du développeur Amazon Simple Queue Service.

Pour pouvoir utiliser la file d'attente Amazon SQS en tant que destination d'une notification d'événements, vous devez disposer des éléments suivants :

- Amazon Resource Name (ARN) de la file d'attente Amazon SQS

> **Note**
>
> Les files d'attente Amazon Simple Queue Service FIFO (premier entré, premier sorti) ne sont pas prises en charge en tant que destination des notifications d'événements Amazon S3. Pour envoyer une notification concernant un événement Amazon S3 à une file d'attente FIFO Amazon SQS, vous pouvez utiliser Amazon. EventBridge Pour de plus amples informations, veuillez consulter Activation d'Amazon EventBridge.

Fonction Lambda

Vous pouvez l'utiliser AWS Lambda pour étendre d'autres AWS services avec une logique personnalisée ou créer votre propre backend qui fonctionne en termes d' AWS échelle, de performances et de sécurité. Lambda vous permet de créer des applications discrètes et axées sur les événements qui ne s'exécutent que lorsque vous en avez besoin. Vous pouvez également l'utiliser pour faire évoluer ces applications automatiquement de quelques requêtes par jour à des milliers de secondes.

Lambda peut exécuter du code personnalisé en réponse aux événements de compartiment Amazon S3 : vous chargez votre code personnalisé dans Lambda et créez ce qu'on appelle une fonction Lambda. Lorsqu'Amazon S3 détecte un événement d'un type spécifique, il peut le publier AWS Lambda et appeler votre fonction dans Lambda. En réponse, Lambda exécute votre fonction. Un type d'événement qu'il peut détecter, par exemple, est un événement créé par un objet.

Vous pouvez utiliser la AWS Lambda console pour créer une fonction Lambda qui utilise l' AWS infrastructure pour exécuter le code en votre nom. La fonction Lambda doit être située dans la même Région que votre compartiment S3. Vous devez également connaître le nom ou l'ARN d'une fonction Lambda pour la configurer en tant que destination de notification d'événements.

> **Warning**
>
> Lorsque votre notification écrit dans le compartiment qui déclenche la notification, cela peut provoquer une boucle d'exécution. Par exemple, si le compartiment déclenche une fonction Lambda chaque fois qu'un objet est chargé et que la fonction charge un objet dans le compartiment, elle 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.
>
> Pour plus d'informations et un exemple d'utilisation des notifications Amazon S3 avec AWS Lambda, consultez la section Utilisation AWS Lambda avec Amazon S3 dans le guide du AWS Lambda développeur.

Amazon EventBridge

Amazon EventBridge est un bus d'événements sans serveur qui reçoit les événements des AWS services. Vous pouvez définir des règles pour faire correspondre les événements et les transmettre à des cibles, par exemple un service AWS ou un point de terminaison HTTP. Pour plus d'informations, consultez le contenu EventBridge du guide de EventBridge l'utilisateur Amazon.

Contrairement aux autres destinations, vous pouvez activer ou désactiver les événements à diffuser EventBridge pour un bucket. Si vous activez la livraison, tous les événements sont envoyés à EventBridge. En outre, vous pouvez utiliser des EventBridge règles pour acheminer les événements vers des cibles supplémentaires.

Types d'événements pris en charge pour SQS, SNS et Lambda

Amazon S3 peut publier les types d'événements ci-après. Vous devez spécifier ces types d'événements dans la configuration des notifications.

Types d'événements	Description
`s3:TestEvent`	Lorsqu'une notification est activée, Amazon S3 publie une notification de test. Cela permet de vérifier que la rubrique existe et que le propriétaire du compartiment est autorisé à publier la rubrique spécifiée. Si l'activation de la notification échoue, vous ne recevez pas de notification de test.

`s3:ObjectCreated:*`
 	
`s3:ObjectCreated:Put`
 	
`s3:ObjectCreated:Post`
 	
`s3:ObjectCreated:Copy`
 	
`s3:ObjectCreated:CompleteMultipartUpload`
	Les opérations d'API Amazon S3 telles que `PUT`, `POST` et `COPY` permettent de créer des objets. Avec ces types d'événements, vous pouvez activer les notifications lorsqu'un objet est créé à l'aide d'une opération API spécifique. Vous pouvez également utiliser le type d'événement `s3:ObjectCreated:*` pour demander une notification quelle que soit l'API utilisée pour créer un objet.
	
	`s3:ObjectCreated:CompleteMultipartUpload` inclut les objets qui sont créés à l'aide d'UploadPartCopy pour les opérations de copie.

`s3:ObjectRemoved:*`
 	
`s3:ObjectRemoved:Delete`
 	
`s3:ObjectRemoved:DeleteMarkerCreated`
	L'utilisation des types d'événements `ObjectRemoved` vous permet d'activer l'envoi de notifications lorsqu'un objet ou un lot d'objets est supprimé d'un compartiment.
	
	Vous pouvez utiliser le type d'événement `s3:ObjectRemoved:Delete` pour demander l'envoi de notificat

Types d'événements	Description
	ions lorsqu'un objet est supprimé ou lorsqu'un objet avec version est supprimé de manière définitive. Vous pouvez également utiliser `s3:ObjectRemoved:DeleteMarkerCreated`, afin de demander l'envoi d'une notification lorsqu'un marqueur de suppression est créé pour un objet avec version. Pour savoir comment supprimer des objets versionnés, consultez Suppression des versions d'objet d'un compartiment activé pour la gestion des versions. Vous pouvez aussi utiliser un caractère générique `s3:ObjectRemoved:*`, afin de demander l'envoi d'une notification chaque fois qu'un objet est supprimé. Ces notifications d'événements ne vous alertent pas lors de suppressions automatiques dans le cadre de configurations de cycle de vie ou lorsque des opérations échouent.

`s3:ObjectRestore:*`
 	
`s3:ObjectRestore:Post`
 	
`s3:ObjectRestore:Completed`
 	
`s3:ObjectRestore:Delete`
	L'utilisation des types d'événements `ObjectRestore` vous permet de recevoir des notifications de début et de fin d'événement lors de la restauration des objets depuis les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive, ou les niveaux d'accès S3 Intelligent-Tiering Archive et S3 Intelligent-Tiering Deep Archive. Vous pouvez également recevoir des notifications lorsque la copie restaurée d'un objet expire.
	
	Le type d'événement `s3:ObjectRestore:Post` vous avertit du début d'une restauration d'objet. Le type d'événement `s3:ObjectRestore:Completed` vous avertit de la fin de la restauration. Le type d'événement `s3:ObjectRestore:Delete` vous avertit lorsque la copie temporaire d'un objet restauré expire.

`s3:ReducedRedundancyLostObject`	Vous recevez cette notification lorsqu'Amazon S3 détecte qu'un objet de la classe de stockage RRS a été perdu.

Types d'événements	Description

`s3:Replication:*`
 	
`s3:Replication:OperationFailedReplication`
 	
`s3:Replication:OperationMissedThreshold`
 	
`s3:Replication:OperationReplicatedAfterThreshold`
 	
`s3:Replication:OperationNotTracked`
	L'utilisation des types d'événements `Replication` vous permet de recevoir des notifications pour les configurations de réplication sur lesquelles des métriques de réplication S3 ou Contrôle du temps de réplication S3 (S3 RTC) sont activées. Vous pouvez surveiller la minute-by-minute progression des événements de réplication en suivant les octets en attente, les opérations en attente et la latence de réplication. Pour plus d'informations sur les métriques de réplication, consultez Surveillance de la réplication avec des métriques, des notifications d'événements et des statuts.
	
	• Le type d'événement `s3:Replication:OperationFailedReplication` vous avertit lorsqu'un objet éligible à la réplication n'a pas pu être répliqué.
	• Le type d'événement `s3:Replication:OperationMissedThreshold` vous avertit lorsqu'un objet éligible à la réplication et qui utilise S3 RTC dépasse le délai maximal de 15 minutes pour la réplication.
	• Le type d'événement `s3:Replication:OperationReplicatedAfterThreshold` vous avertit lorsqu'un objet éligible à la réplication et qui utilise S3 RTC est répliqué après le délai maximal de 15 minutes.
	• Le type d'événement `s3:Replication:OperationNotTracked` vous avertit lorsqu'un objet éligible à la réplication en direct (réplication sur une même région [SRR] ou réplication interrégionale [CRR]) n'est plus suivi par les métriques de réplication.

Types d'événements	Description

`s3:LifecycleExpiration:*`
 	
`s3:LifecycleExpiration:Delete`
 	
`s3:LifecycleExpiration:DeleteMarkerCreated`
	Avec les types d'événements `LifecycleExpiration` , vous pouvez recevoir une notification lorsqu'Amazon S3 supprime un objet en fonction de votre configuration de cycle de vie S3.
	
	Le type d'événement `s3:LifecycleExpiration:Delete` vous avertit lorsqu'un objet dans un compartiment non versionné est supprimé. Il vous avertit également lorsqu'une version d'objet est définitivement supprimée par une configuration de cycle de vie S3. Le type d'événement `s3:LifecycleExpiration:DeleteMarkerCreated` vous avertit lorsque le cycle de vie S3 crée un marqueur de suppression lors de la suppression d'une version actuelle d'un objet dans un compartiment versionné.

`s3:LifecycleTransition`	Vous recevez cette notification d'événement lorsqu'un objet est transféré vers une autre classe de stockage Amazon S3 par une configuration de cycle de vie S3.
`s3:IntelligentTiering`	Vous recevez cette notification d'événement afin d'être informé lorsqu'un objet de la classe de stockage S3 Intelligent-Tiering est passé au niveau d'accès Archive ou au niveau d'accès Deep Archive.

`s3:ObjectTagging:*`
 	
`s3:ObjectTagging:Put`
 	
`s3:ObjectTagging:Delete`
	L'utilisation des types d'événements `ObjectTagging` vous permet d'activer l'envoi de notifications lorsqu'une balise d'objet est ajoutée ou supprimée d'un objet.
	
	Le type d'événement `s3:ObjectTagging:Put` vous avertit lorsqu'une étiquette est PUT sur un objet ou qu'une étiquette existante est mise à jour. Le type d'événement `s3:ObjectTagging:Delete` vous avertit lorsqu'une étiquette est supprimée d'un objet.

Types d'événements	Description
`s3:ObjectAcl:Put`	Vous recevez cette notification d'événement lorsqu'une liste ACL est PUT sur un objet ou lorsqu'une liste ACL existante est modifiée. Un événement n'est pas généré lorsqu'une demande n'entraîne aucune modification de la liste ACL d'un objet.

Types d'événements pris en charge pour Amazon EventBridge

Pour obtenir la liste des types d'événements qu'Amazon S3 enverra à Amazon EventBridge, consultezEn utilisant EventBridge.

Ordre des événements et doublons

Les notifications d'événements Amazon S3 sont conçues pour envoyer des notifications au moins une fois, mais il n'est pas garanti qu'elles arrivent dans le même ordre que celui dans lequel les événements se sont produits. Dans de rares cas, le mécanisme de nouvelle tentative d'Amazon S3 peut provoquer des notifications d'événement S3 dupliquées pour le même événement d'objet. Pour en savoir plus sur la gestion des événements dupliqués ou des événements qui ne sont pas notifiés dans l'ordre, consultez Gestion de l'ordre des événements et des événements dupliqués avec les notifications d'événements Amazon S3 dans le blog AWS Storage.

Utilisation d'Amazon SQS, Amazon SNS et Lambda

L'activation des notifications s'effectue au niveau du compartiment. Vous stockez les informations de configuration de la notification dans la sous-ressource notification qui est associée à un compartiment. Après avoir créé ou modifié la configuration de notification du compartiment, il faut généralement attendre 5 minutes pour que les modifications prennent effet. Lorsque la notification est activée pour la première fois, un événement `s3:TestEvent` se produit. Suivez l'une des méthodes suivantes pour gérer la configuration des notifications :

- Via la console Amazon S3 – Vous pouvez utilisez l'interface de la console pour définir une configuration de notifications pour un compartiment sans écrire de code. Pour de plus amples informations, veuillez consulter Activation et configuration des notifications d'événements à l'aide de la console Amazon S3.
- À l'aide de la programmation AWS SDKs : en interne, à la fois la console et l' SDKs appel de l'API REST Amazon S3 pour gérer les sous-ressources de notification associées au compartiment.

Pour des exemples de configuration des notifications qui utilisent le kit AWS SDK, consultez Démonstration : configuration d'un compartiment pour les notifications (rubrique SNS ou file d'attente SQS).

> **Note**
>
> Vous pouvez aussi appeler l'API REST Amazon S3 directement depuis votre code. Toutefois, cette méthode peut s'avérer fastidieuse, car vous devez écrire du code pour authentifier vos demandes.

Quelle que soit la méthode que vous utilisez, Amazon S3 stocke la configuration des notifications au format XML dans la sous-ressource notification qui est associée au compartiment. Pour plus d'informations sur les sous-ressources de compartiment, consultez Options de configuration des buckets à usage général.

> **Note**
>
> Si vous recevez plusieurs notifications d'échec d'événement dues à la suppression de destinations, vous pouvez recevoir le message Unable to validate the following destination configurations (Impossible de valider les configurations de destination suivantes) lorsque vous essayez de les supprimer. Vous pouvez résoudre ce problème dans la console S3 en supprimant simultanément toutes les notifications d'échec.

Rubriques

- Octroi d'autorisations pour la publication de messages de notification d'événement vers une destination
- Activation et configuration des notifications d'événements à l'aide de la console Amazon S3
- Configuration des notifications d'événements par programmation
- Démonstration : configuration d'un compartiment pour les notifications (rubrique SNS ou file d'attente SQS)
- Configuration des notifications d'événement à l'aide du filtrage des noms de clé d'objet
- Structure des messages d'événements

Octroi d'autorisations pour la publication de messages de notification d'événement vers une destination

Vous devez accorder au principal Amazon S3 les autorisations nécessaires pour appeler l'API appropriée afin de publier des messages dans une rubrique SNS, une file d'attente SQS ou une fonction Lambda. Amazon S3 peut ainsi publier des messages de notification d'événement vers une destination.

Pour résoudre les problèmes liés à la publication de messages de notification d'événements vers une destination, consultez Troubleshoot to publish Amazon S3 event notifications to an Amazon Simple Notification Service topic (Résoudre les problèmes liés à la publication de notifications d'événements Amazon S3 sur une rubrique Amazon Simple Notification Service).

Rubriques

- Octroi d'autorisations pour appeler une AWS Lambda fonction
- Octroi d'autorisations pour la publication de messages dans une rubrique SNS ou une file d'attente SQS

Octroi d'autorisations pour appeler une AWS Lambda fonction

Amazon S3 publie des messages d'événement sur AWS Lambda en invoquant une fonction Lambda et en fournissant le message d'événement comme argument.

Lorsque vous utilisez la console Amazon S3 pour configurer les notifications d'événements sur un compartiment Amazon S3 pour une fonction Lambda, la console définit les autorisations nécessaires au niveau de la fonction Lambda. Amazon S3 dispose ainsi d'autorisations pour invoquer la fonction à partir du compartiment. Pour de plus amples informations, veuillez consulter Activation et configuration des notifications d'événements à l'aide de la console Amazon S3.

Vous pouvez également accorder à Amazon S3 des autorisations AWS Lambda pour appeler votre fonction Lambda. Pour plus d'informations, consultez Tutoriel : Utilisation AWS Lambda avec Amazon S3 dans le Guide du AWS Lambda développeur.

Octroi d'autorisations pour la publication de messages dans une rubrique SNS ou une file d'attente SQS

Pour accorder à Amazon S3 l'autorisation de publier des messages sur la rubrique SNS ou la file d'attente SQS, associez une politique AWS Identity and Access Management (IAM) à la rubrique SNS ou à la file d'attente SQS de destination.

Pour afficher un exemple montrant comment associer une stratégie à une rubrique SNS ou à une file d'attente SQS, consultez Démonstration : configuration d'un compartiment pour les notifications (rubrique SNS ou file d'attente SQS). Pour en savoir plus sur les autorisations, consultez les rubriques suivantes :

- Cas d'utilisation du contrôle des accès Amazon SNS dans le Manuel du développeur Amazon Simple Notification Service
- Identity and Access Management dans Amazon SQS dans le Manuel du développeur Amazon Simple Queue Service

Politique IAM pour une rubrique SNS de destination

Voici un exemple de stratégie AWS Identity and Access Management (IAM) que vous associez à la rubrique SNS de destination. Pour savoir comment utiliser cette politique pour configurer une rubrique Amazon SNS de destination pour les notifications d'événements, consultez Démonstration : configuration d'un compartiment pour les notifications (rubrique SNS ou file d'attente SQS).

JSON

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "Example SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "arn:aws:sns:aws-region:111122223333:example-sns-topic",
            "Condition": {
                "ArnEquals": {
                    "aws:SourceArn": "arn:aws:s3:::amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
```

```
            }
        }
    ]
}
```

Politique IAM pour une file d'attente SQS de destination

Voici un exemple de politique IAM que vous associez à la file d'attente SQS de destination. Pour savoir comment utiliser cette politique pour configurer une file d'attente Amazon SQS de destination pour les notifications d'événements, consultez Démonstration : configuration d'un compartiment pour les notifications (rubrique SNS ou file d'attente SQS).

Pour utiliser cette politique, vous devez mettre à jour l'ARN de la file d'attente Amazon SQS, le nom du bucket et l'ID du propriétaire du Compte AWS bucket.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "arn:aws:sqs:us-east-1:111122223333:queue-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
```

```
}
```

Qu'il s'agisse de la politique IAM Amazon SNS ou de la politique IAM Amazon SQS, vous pouvez spécifier la condition `StringLike` en lieu et place de la condition `ArnLike` dans la stratégie.

Lorsque `ArnLike` est utilisé, les parties partition, service, ID de compte, type de ressource et ID de ressource partiel de l'ARN doivent correspondre exactement à l'ARN dans le contexte de la demande. Seuls la région et le chemin de ressource permettent une correspondance partielle.

Lorsque `StringLike` est utilisé à la place de `ArnLike`, la correspondance ignore la structure de l'ARN et permet une correspondance partielle, quelle que soit la partie qui a été marquée par un caractère générique. Pour plus d'informations, consultez Éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

```
"Condition": {
  "StringLike": { "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket" }
  }
```

AWS KMS politique clé

Si la file d'attente SQS ou les sujets SNS sont chiffrés à l'aide d'une clé gérée par le client AWS Key Management Service (AWS KMS), vous devez accorder au principal du service Amazon S3 l'autorisation d'utiliser les sujets ou la file d'attente chiffrés. Ajoutez l'instruction suivante à la politique de la clé gérée par le client afin d'accorder l'autorisation au principal de service Amazon S3.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
```

```
                "kms:Decrypt"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur les politiques AWS KMS clés, consultez la section Utilisation des politiques clés AWS KMS dans le Guide du AWS Key Management Service développeur.

Pour plus d'informations sur l'utilisation du chiffrement côté serveur AWS KMS pour Amazon SQS et Amazon SNS, consultez ce qui suit :

- Gestion des clés dans le Manuel du développeur Amazon Simple Notification Service.
- Gestion des clés dans le Manuel du développeur Amazon Simple Queue Service.
- Chiffrement des messages publiés vers Amazon SNS avec AWS KMS dans le Blog sur le calcul AWS .

Activation et configuration des notifications d'événements à l'aide de la console Amazon S3

Vous pouvez activer certains événements de compartiment à usage général Amazon S3 pour envoyer un message de notification à une destination chaque fois que ces événements se produisent. Cette section explique comment utiliser la console Amazon S3 pour activer les notifications d'événement. Pour plus d'informations sur l'utilisation des notifications d'événements avec le REST AWS SDKs et Amazon S3 APIs, consultezConfiguration des notifications d'événements par programmation.

Prérequis : avant de pouvoir activer les notifications d'événements pour votre compartiment, vous devez configurer l'un des types de destination, puis configurer les autorisations. Pour plus d'informations, consultez Destinations d'événements prises en charge et Octroi d'autorisations pour la publication de messages de notification d'événement vers une destination.

> **Note**
>
> Les files d'attente Amazon Simple Queue Service FIFO (premier entré, premier sorti) ne sont pas prises en charge en tant que destination des notifications d'événements Amazon S3. Pour envoyer une notification concernant un événement Amazon S3 à une file d'attente FIFO

Amazon SQS, vous pouvez utiliser Amazon. EventBridge Pour de plus amples informations, veuillez consulter Activation d'Amazon EventBridge.

Rubriques

- Activation des notifications Amazon SNS, Amazon SQS ou Lambda à l'aide de la console Amazon S3

Activation des notifications Amazon SNS, Amazon SQS ou Lambda à l'aide de la console Amazon S3

Pour activer et configurer des notifications d'événements pour un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer les événements.
4. Choisissez Propriétés.
5. Accédez à la section Event Notifications (Notifications d'événements) et choisissez Create event notification (Créer une notification d'événements).
6. Dans la section General configuration (Configuration générale) spécifiez le nom d'événement descriptif pour votre notification d'événements. Vous pouvez également spécifier un préfixe et un suffixe pour limiter les notifications aux objets dont les clés se terminent par les caractères spécifiés.

   a. Saisissez une description pour Event name (Nom de l'événement).

      Si vous ne saisissez pas de nom, un identifiant unique global (GUID) sera généré et utilisé pour le nom.

   b. (Facultatif) Pour filtrer les notifications d'événements par préfixe, saisissez un préfixe.

      Par exemple, vous pouvez configurer un filtre de préfixe de sorte à recevoir uniquement des notifications lorsque des fichiers sont ajoutés à un dossier spécifique (par exemple, `images/`).

   c. (Facultatif) Pour filtrer les notifications d'événements par suffixe, saisissez un suffixe.

Pour plus d'informations, consultez Configuration des notifications d'événement à l'aide du filtrage des noms de clé d'objet.

7. Dans la section Event types (Types d'événements), sélectionnez un ou plusieurs types d'événements pour lesquels vous souhaitez recevoir des notifications.

   Pour obtenir la liste des différents types d'événements, consultez Types d'événements pris en charge pour SQS, SNS et Lambda.

8. Dans la section Destination choisissez la destination de notification d'événements.

   > **Note**
   >
   > Avant de publier des notifications d'événements, vous devez accorder au principal Amazon S3 les autorisations requises pour qu'il puisse appeler l'API pertinente. Il peut ainsi publier des notifications vers une fonction Lambda, une rubrique SNS ou une file d'attente SQS.

   a. Sélectionnez le type de destination : Lambda Function (Fonction Lambda), SNS Topic (Rubrique SNS) ou SQS Queue (File d'attente SQS).

   b. Après avoir choisi votre type de destination, choisissez une fonction, une rubrique ou une file d'attente dans la liste.

   c. Si vous préférez spécifier un Amazon Resource Name (ARN), utilisez l'option Saisir l'ARN.

   Pour plus d'informations, consultez Destinations d'événements prises en charge.

9. Choisissez Enregistrer les modifications. Amazon S3 envoie alors un message de test à la destination de notification d'événements.

Configuration des notifications d'événements par programmation

Par défaut, les notifications sont désactivées pour tous les types d'événements. Par conséquent, la sous-ressource notification stocke initialement une configuration vide.

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
</NotificationConfiguration>
```

Pour activer les notifications pour certains types d'événements, vous devez remplacer le fichier XML par la configuration appropriée, qui identifie les types d'événements que doit publier Amazon S3, ainsi que leurs destinations. Vous devez ajouter une configuration XML pour chaque destination.

Publication des messages d'événement dans une file d'attente SQS

Pour définir une file d'attente SQS comme destination de notification pour un ou plusieurs types d'événements, ajoutez l'élément `QueueConfiguration`.

```
<NotificationConfiguration>
  <QueueConfiguration>
    <Id>optional-id-string</Id>
    <Queue>sqs-queue-arn</Queue>
    <Event>event-type</Event>
    <Event>event-type</Event>
     ...
  </QueueConfiguration>
   ...
</NotificationConfiguration>
```

Publication des messages d'événement dans une rubrique SNS

Pour définir une rubrique SNS comme destination de notification pour des types d'événements spécifiques, ajoutez l'élément `TopicConfiguration`.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>optional-id-string</Id>
     <Topic>sns-topic-arn</Topic>
     <Event>event-type</Event>
     <Event>event-type</Event>
      ...
  </TopicConfiguration>
   ...
</NotificationConfiguration>
```

Pour appeler la AWS Lambda fonction et fournir un message d'événement en tant qu'argument

Pour définir une fonction Lambda comme destination de notification pour des types d'événements spécifiques, ajoutez l'élément `CloudFunctionConfiguration`.

```
<NotificationConfiguration>
```

```
  <CloudFunctionConfiguration>
     <Id>optional-id-string</Id>
     <CloudFunction>cloud-function-arn</CloudFunction>
     <Event>event-type</Event>
     <Event>event-type</Event>
      ...
  </CloudFunctionConfiguration>
   ...
</NotificationConfiguration>
```

Suppression de toute les notifications configurées pour un compartiment

Pour supprimer toutes les notifications configurées pour un compartiment, enregistrez un élément `<NotificationConfiguration/>` vide dans la sous-ressource notification.

Lorsque Amazon S3 détecte un événement qui appartient au type spécifié, il publie un message contenant les informations relatives à cet événement. Pour plus d'informations, consultez Structure des messages d'événements.

Pour plus d'informations sur la configuration des notifications d'événements, consultez les rubriques suivantes :

- Démonstration : configuration d'un compartiment pour les notifications (rubrique SNS ou file d'attente SQS).
- Configuration des notifications d'événement à l'aide du filtrage des noms de clé d'objet

Démonstration : configuration d'un compartiment pour les notifications (rubrique SNS ou file d'attente SQS)

Vous pouvez recevoir des notifications Amazon S3 à l'aide d'Amazon Simple Notification Service (Amazon SNS) ou d'Amazon Simple Queue Service (Amazon SQS). Dans le cadre de cette démonstration, vous allez ajouter une configuration de notification à votre compartiment à l'aide d'une rubrique Amazon SNS et d'une file d'attente Amazon SQS.

> **Note**
>
> Les files d'attente Amazon Simple Queue Service FIFO (premier entré, premier sorti) ne sont pas prises en charge en tant que destination des notifications d'événements Amazon S3. Pour envoyer une notification concernant un événement Amazon S3 à une file d'attente FIFO

Amazon SQS, vous pouvez utiliser Amazon. EventBridge Pour de plus amples informations, veuillez consulter Activation d'Amazon EventBridge.

Rubriques

- Résumé de la procédure détaillée
- Étape 1 : créer une file d'attente Amazon SQS
- Étape 2 : créer une rubrique Amazon SNS
- Étape 3 : ajouter une configuration de notifications à votre compartiment
- Étape 4 : tester la configuration

Résumé de la procédure détaillée

Cette démonstration vous explique comment :

- Publier des événements de type `s3:ObjectCreated:*` dans une file d'attente Amazon SQS.
- Publier des événements de type `s3:ReducedRedundancyLostObject` dans une rubrique Amazon SNS.

Pour en savoir plus sur la configuration des notifications, consultez Utilisation d'Amazon SQS, Amazon SNS et Lambda.

Vous pouvez suivre toutes ces étapes via la console sans écrire de code. En outre, des exemples de code utilisés AWS SDKs pour Java et .NET sont également fournis pour vous aider à ajouter des configurations de notification par programmation.

La procédure comprend les étapes suivantes :

1. Créez une file d'attente Amazon SQS.

   Via la console Amazon SQS, créez un file d'attente. Vous pouvez accéder par programmation à tous les messages qu'Amazon S3 envoie vers la file d'attente. Mais dans le cadre de cette procédure détaillée, vous vérifierez tous les messages de notification sur la console.

   Vous associez une stratégie d'accès à la file d'attente afin d'autoriser Amazon S3 à publier des messages.
2. Créez une rubrique Amazon SNS.

À l'aide de la console Amazon SNS, créez une rubrique SNS et abonnez-y. Ainsi, tout événement publié dans cette rubrique vous est signalé. Vous définissez l'e-mail comme protocole de communication. Lorsque vous créez une rubrique, Amazon SNS vous envoie un e-mail. Vous suivez le lien contenu dans l'e-mail pour confirmer votre abonnement à la rubrique.

Vous associez une stratégie d'accès à la rubrique, afin d'autoriser Amazon S3 à publier des messages.

3. Ajouter une configuration de notifications à un compartiment.

Étape 1 : créer une file d'attente Amazon SQS

Suivez les étapes pour créer une file d'attente Amazon Simple Queue Service (Amazon SQS) et vous y abonner.

1. À l'aide de la console Amazon SQS, créez une file d'attente. Pour obtenir des instructions, consultez Démarrez avec Amazon SQS dans le Manuel du développeur Amazon Simple Queue Service.
2. Remplacez la stratégie d'accès qui est associée à la file d'attente par la stratégie ci-après.
   a. Dans la console Amazon SQS, dans la liste Queues (Files d'attente), sélectionnez le nom de la file d'attente.
   b. Dans l'onglet Access policy (Stratégie d'accès), choisissez Edit (Modifier).
   c. Remplacez la stratégie d'accès qui est associée à la file d'attente. Indiquez votre ARN Amazon SQS, le nom du compartiment source et l'ID de compte du propriétaire du compartiment.

      JSON

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
```

```
            },
            "Action": [
                "SQS:SendMessage"
            ],
            "Resource": "arn:aws:sqs:us-west-2:111122223333:s3-
notification-queue",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:awsexamplebucket1"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

d. Choisissez Enregistrer.

3. (Facultatif) Si le chiffrement côté serveur est activé AWS Key Management Service avec AWS KMS() dans la file d'attente Amazon SQS ou dans la rubrique Amazon SNS, ajoutez la politique suivante à la clé de chiffrement symétrique gérée par le client associée.

   Vous devez ajouter la politique à une clé gérée par le client, car vous ne pouvez pas modifier la clé gérée par AWS pour Amazon SQS ou Amazon SNS.

   JSON

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "example-statement-ID",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "kms:GenerateDataKey",
                "kms:Decrypt"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur l'utilisation de SSE pour Amazon SQS et Amazon SNS AWS KMS avec, consultez ce qui suit :

- Gestion des clés dans le Manuel du développeur Amazon Simple Notification Service.
- Gestion des clés dans le Manuel du développeur Amazon Simple Queue Service.

4. Notez l'ARN de la file d'attente.

   La file d'attente SQS que vous avez créée est une autre ressource dans votre Compte AWS. Elle possède un Amazon Resource Name (ARN) unique. Vous avez besoin de cet ARN à la prochaine étape. L'ARN présente dans le format suivant :

   ```
   arn:aws:sqs:aws-region:account-id:queue-name
   ```

Étape 2 : créer une rubrique Amazon SNS

Suivez ces étapes pour créer une rubrique Amazon SNS et vous y abonner.

1. Créez une rubrique à partir de la console Amazon SNS. Des instructions sont disponibles dans la section Création d'une rubrique Amazon SNS du Manuel du développeur Amazon Simple Notification Service.
2. Abonnez-vous à la rubrique. Dans le cadre de cet exercice, définissez l'e-mail comme protocole de communication. Pour obtenir des instructions, consultez Abonnement à une rubrique Amazon SNS dans le Manuel du développeur Amazon Simple Notification Service.

   Vous recevez un e-mail vous invitant à confirmer votre abonnement à la rubrique. Confirmez votre abonnement.
3. Remplacez la stratégie d'accès associée à la rubrique par la stratégie ci-après. Indiquez l'ARN de votre rubrique SNS, le nom du compartiment et l'ID de compte du propriétaire du compartiment.

JSON

```
{
    "Version": "2012-10-17",
    "Id": "example-ID",
    "Statement": [
        {
            "Sid": "Example SNS topic policy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": [
                "SNS:Publish"
            ],
            "Resource": "arn:aws:sns:aws-region:111122223333:topic-name",
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:*:*:amzn-s3-demo-bucket"
                },
                "StringEquals": {
                    "aws:SourceAccount": "bucket-owner-account-id"
                }
            }
        }
    ]
}
```

4. Notez l'ARN de la rubrique.

   La rubrique SNS que vous avez créée est une autre ressource de votre Compte AWS choix, et elle possède un ARN unique. Vous aurez besoin de cet ARN à la prochaine étape. L'ARN présentera le format suivant :

   ```
   arn:aws:sns:aws-region:account-id:topic-name
   ```

Étape 3 : ajouter une configuration de notifications à votre compartiment

Vous pouvez activer les notifications de compartiment à l'aide de la console Amazon S3 ou par programmation à l'aide de. AWS SDKs Choisissez l'une des deux méthodes pour configurer les

notifications de votre compartiment. Cette section fournit des exemples de code utilisant AWS SDKs pour Java et .NET.

Option A : Activer des notifications d'un compartiment via la console

Dans la console Amazon S3, ajoutez une configuration de notifications demandant à Amazon S3 de :

- Publier les événements du type All objet create events (Tous les événements de création d'objet) dans votre file d'attente Amazon SQS.
- Publier les événements du type Object in RRS lost (Objet dans le stockage Reduced Redundancy Storage (RRS) perdu) dans votre rubrique Amazon SNS.

Une fois que vous avez enregistré la configuration de notifications, Amazon S3 publie un message de test, que vous recevez par e-mail.

Pour obtenir des instructions, veuillez consulter Activation et configuration des notifications d'événements à l'aide de la console Amazon S3.

Option B : activer les notifications sur un compartiment à l'aide du AWS SDKs

.NET

L'exemple de code C# ci-dessous fournit une liste complète de codes qui permet d'ajouter une configuration de notifications à un compartiment. Vous devez mettre à jour le code et fournir le nom de votre compartiment, ainsi que l'ARN de la rubrique SNS. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class EnableNotificationsTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string snsTopic = "*** SNS topic ARN ***";
```

```
        private const string sqsQueue = "*** SQS topic ARN ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
RegionEndpoint.USWest2;
        private static IAmazonS3 client;

        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            EnableNotificationAsync().Wait();
        }

        static async Task EnableNotificationAsync()
        {
            try
            {
               PutBucketNotificationRequest request = new
PutBucketNotificationRequest
                {
                    BucketName = bucketName
                };

                TopicConfiguration c = new TopicConfiguration
                {
                    Events = new List<EventType> { EventType.ObjectCreatedCopy },
                    Topic = snsTopic
                };
                request.TopicConfigurations = new List<TopicConfiguration>();
                request.TopicConfigurations.Add(c);
                request.QueueConfigurations = new List<QueueConfiguration>();
                request.QueueConfigurations.Add(new QueueConfiguration()
                {
                    Events = new List<EventType> { EventType.ObjectCreatedPut },
                    Queue = sqsQueue
                });

                PutBucketNotificationResponse response = await
client.PutBucketNotificationAsync(request);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' ",
e.Message);
            }
```

```
            catch (Exception e)
            {
                Console.WriteLine("Unknown error encountered on server.
 Message:'{0}' ", e.Message);
            }
        }
    }
}
```

Java

L'exemple suivant montre comment ajouter une configuration de notification à un compartiment. Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, consultez Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.io.IOException;
import java.util.EnumSet;

public class EnableNotificationOnABucket {

    public static void main(String[] args) throws IOException {
        String bucketName = "*** Bucket name ***";
        Regions clientRegion = Regions.DEFAULT_REGION;
        String snsTopicARN = "*** SNS Topic ARN ***";
        String sqsQueueARN = "*** SQS Queue ARN ***";

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();
            BucketNotificationConfiguration notificationConfiguration = new
 BucketNotificationConfiguration();
```

```
            // Add an SNS topic notification.
            notificationConfiguration.addConfiguration("snsTopicConfig",
                    new TopicConfiguration(snsTopicARN,
 EnumSet.of(S3Event.ObjectCreated)));

            // Add an SQS queue notification.
            notificationConfiguration.addConfiguration("sqsQueueConfig",
                    new QueueConfiguration(sqsQueueARN,
 EnumSet.of(S3Event.ObjectCreated)));

            // Create the notification configuration request and set the bucket
 notification
            // configuration.
            SetBucketNotificationConfigurationRequest request = new
 SetBucketNotificationConfigurationRequest(
                    bucketName, notificationConfiguration);
            s3Client.setBucketNotificationConfiguration(request);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Étape 4 : tester la configuration

Vous pouvez désormais tester la configuration. Pour ce faire, chargez un objet vers votre compartiment et vérifiez la notification d'événement dans la console Amazon SQS. Pour obtenir des instructions, consultez Recevez et supprimez votre message dans la section « Mise en route » du Manuel du développeur Amazon Simple Queue Service.

Configuration des notifications d'événement à l'aide du filtrage des noms de clé d'objet

Lorsque vous configurez une notification d'événements Amazon S3, vous devez spécifier quels types d'événements Amazon S3 pris en charge entraînent l'envoi de la notification par Amazon S3. Si un

type d'événement que vous n'avez pas spécifié se produit dans votre compartiment S3, Amazon S3 n'envoie pas de notification.

Vous pouvez configurer les notifications pour qu'elles soient filtrées en fonction du préfixe et du suffixe du nom de clé des objets. Par exemple, vous pouvez définir une configuration afin de ne recevoir une notification uniquement lorsque des fichiers image comportant l'extension de nom de fichier « `.jpg` » sont ajoutés à un compartiment. Vous pouvez également avoir une configuration qui envoie une notification à une rubrique Amazon SNS lorsqu'un objet avec le préfixe « `images/` » est ajouté au compartiment, tandis que des notifications pour les objets ayant un préfixe « `logs/` » dans le même compartiment sont envoyées à une fonction. AWS Lambda

> **Note**
>
> Les filtres n'acceptent pas de caractère générique (« * ») comme préfixe ou suffixe. Si votre préfixe ou suffixe contient un espace, vous devez le remplacer par le caractère « + ». Si vous utilisez un autre caractère spécial dans la valeur du préfixe ou du suffixe, vous devez les entrer au format codé en URL (encodage-pourcent). Pour obtenir la liste complète des caractères spéciaux qui doivent être convertis en format codé URL lorsqu'ils sont utilisés dans un préfixe ou un suffixe pour les notifications d'événements, consultez Caractères adaptés.

Ces configurations de notifications en fonction du nom de clé d'objet peuvent être définies dans la console Amazon S3. Vous pouvez le faire en utilisant Amazon S3 APIs via le REST AWS SDKs ou APIs directement. Pour en savoir plus sur l'utilisation de l'interface utilisateur de la console pour définir une configuration de notification pour un compartiment, consultez Activation et configuration des notifications d'événements à l'aide de la console Amazon S3.

Amazon S3 stocke la configuration des notifications au format XML dans la sous-ressource notification associée à un compartiment, comme décrit dans Utilisation d'Amazon SQS, Amazon SNS et Lambda. Pour définir les règles de filtrage des notifications en fonction du préfixe ou du suffixe du nom clé de l'objet, utilisez la structure XML `Filter`. Pour plus d'informations sur la structure XML `Filter`, consultez PUT Bucket notification dans la Référence d'API Amazon Simple Storage Service.

Lorsque les configurations de notifications utilisent `Filter`, les règles de filtrage ne doivent pas contenir de préfixes qui se chevauchent, de suffixes qui se chevauchent, ni de préfixes et suffixes qui se chevauchent. Les sections suivantes contiennent des exemples de configurations de

notification valides avec filtrage des noms de clé d'objet. Elles proposent également des exemples de configurations de notification non valides en raison du chevauchement des préfixes et des suffixes.

Rubriques

- Exemples corrects de configurations des notifications avec filtrage par nom de clé d'objet
- Exemples de configurations des notifications avec chevauchement incorrect des préfixes et des suffixes

Exemples corrects de configurations des notifications avec filtrage par nom de clé d'objet

La configuration des notifications ci-après comporte une configuration de file d'attente qui identifie une file d'attente Amazon SQS dans laquelle Amazon S3 doit publier les événements de type `s3:ObjectCreated:Put`. Les événements sont publiés chaque fois qu'un objet présentant un préfixe `images/` et un suffixe `jpg` est ajouté dans un compartiment via une demande PUT.

```
<NotificationConfiguration>
  <QueueConfiguration>
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>images/</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>jpg</Value>
              </FilterRule>
          </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:s3notificationqueue</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

La configuration de notifications ci-dessous comporte plusieurs préfixes qui ne se chevauchent pas. La configuration indique que les notifications associées aux demandes PUT du dossier `images/` sont envoyées vers une file d'attente A (queue-A), alors que les notifications associées aux demandes PUT du dossier `logs/` sont envoyées vers une file d'attente B (queue-B).

```
<NotificationConfiguration>
  <QueueConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images/</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-A</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
  <QueueConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>logs/</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <Queue>arn:aws:sqs:us-west-2:444455556666:sqs-queue-B</Queue>
     <Event>s3:ObjectCreated:Put</Event>
  </QueueConfiguration>
</NotificationConfiguration>
```

La configuration de notifications ci-dessous comporte plusieurs suffixes qui ne se chevauchent pas. La configuration définit que toutes les `.jpg` images récemment ajoutées au bucket sont traitées par Lambda cloud-function-A, et que toutes les `.png` images récemment ajoutées sont traitées par. cloud-function-B Les `.jpg` suffixes `.png` et ne se chevauchent pas même s'ils ont la même dernière lettre. Si une chaîne donnée peut se terminer par deux suffixes, on considère que les deux suffixes se chevauchent. Une chaîne ne pouvant se terminer par `.png` et `.jpg`, les suffixes de cet exemple de configuration ne se chevauchent pas.

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
```

```
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

Lorsque vos configurations de notifications utilisent `Filter`, les règles de filtrage associées à des types d'événements identiques ne doivent pas contenir de préfixes qui se chevauchent. Ils ne peuvent le faire que si les préfixes qui se chevauchent sont utilisés avec des suffixes qui ne se chevauchent pas. Dans l'exemple de configuration ci-dessous, nous voyons que des objets créés avec un préfixe commun, mais dont les suffixes ne se chevauchent pas, peuvent être envoyés vers différentes destinations.

```
<NotificationConfiguration>
  <CloudFunctionConfiguration>
     <Id>1</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
```

```
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.jpg</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-A</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
  <CloudFunctionConfiguration>
     <Id>2</Id>
     <Filter>
            <S3Key>
                <FilterRule>
                    <Name>prefix</Name>
                    <Value>images</Value>
                </FilterRule>
                <FilterRule>
                    <Name>suffix</Name>
                    <Value>.png</Value>
                </FilterRule>
            </S3Key>
     </Filter>
     <CloudFunction>arn:aws:lambda:us-west-2:444455556666:cloud-function-B</
CloudFunction>
     <Event>s3:ObjectCreated:Put</Event>
  </CloudFunctionConfiguration>
</NotificationConfiguration>
```

Exemples de configurations des notifications avec chevauchement incorrect des préfixes et des suffixes

Lorsque vos configurations de notifications utilisent `Filter`, dans la majorité des cas, les règles de filtrage associées à des types d'événements identiques ne doivent pas contenir de préfixes qui se chevauchent, de suffixes qui se chevauchent, ni de combinaisons de préfixes et de suffixes qui se chevauchent. Elles peuvent toutefois comporter des préfixes qui se chevauchent, à condition que les suffixes ne se chevauchent pas. Pour obtenir un exemple, consultez Configuration des notifications d'événement à l'aide du filtrage des noms de clé d'objet.

En revanche, il est possible d'utiliser des filtres par nom de clé d'objet qui se chevauchent lorsque les types d'événements sont différents. Par exemple, vous pouvez créer une configuration de

notifications qui utilise le préfixe `image/` pour le type d'événement `ObjectCreated:Put` et le préfixe `image/` pour le type d'événement `ObjectRemoved:*`.

Que vous utilisiez la console Amazon S3 ou l'API, si vous tentez d'enregistrer une configuration des notifications comportant des filtres de nom non valides qui se chevauchent pour les mêmes types d'événements, vous obtenez un message d'erreur. Cette section présente des exemples de configurations des notifications incorrectes, en raison du chevauchement des filtres de nom.

Toute règle de configuration des notifications existante est supposée comporter un préfixe et un suffixe par défaut qui correspondent respectivement à n'importe quel autre préfixe et suffixe. La configuration des notifications ci-dessous est incorrecte, car elle comporte des préfixes qui se chevauchent. Plus précisément, le préfixe racine chevauche n'importe quel autre préfixe. Cela est également vrai si, dans cet exemple, vous utilisiez un suffixe en lieu et place d'un préfixe. Le suffixe racine chevaucherait également n'importe quel autre suffixe.

```
<NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-notification-two</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>prefix</Name>
                     <Value>images</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration>
```

La configuration des notifications ci-dessous est incorrecte, car elle comporte des suffixes qui se chevauchent. Si une chaîne donnée peut se terminer par deux suffixes, on considère que les deux suffixes se chevauchent. Une chaîne peut se terminer par `jpg` et `pg`. Ainsi, les suffixes se chevauchent. Il en va de même pour les préfixes. Si une chaîne donnée peut commencer par deux préfixes, on considère que les deux préfixes se chevauchent.

```
 <NotificationConfiguration>
```

```
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
         <Event>s3:ObjectCreated:Put</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>pg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration
```

La configuration des notifications ci-dessous est incorrecte, car elle comporte des préfixes et des suffixes qui se chevauchent.

```
<NotificationConfiguration>
     <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-one</Topic>
         <Event>s3:ObjectCreated:*</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>prefix</Name>
                     <Value>images</Value>
                 </FilterRule>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
```

```
            </S3Key>
        </Filter>
    </TopicConfiguration>
    <TopicConfiguration>
         <Topic>arn:aws:sns:us-west-2:444455556666:sns-topic-two</Topic>
         <Event>s3:ObjectCreated:Put</Event>
         <Filter>
             <S3Key>
                 <FilterRule>
                     <Name>suffix</Name>
                     <Value>jpg</Value>
                 </FilterRule>
            </S3Key>
        </Filter>
    </TopicConfiguration>
</NotificationConfiguration>
```

Structure des messages d'événements

Le message de notification qu'envoie Amazon S3 pour publier un événement est au format JSON.

Pour obtenir une présentation générale et des instructions sur la configuration des notifications d'événement, consultez Notifications d'événements Amazon S3.

Cet exemple illustre la version 2.2 de la structure JSON de notification d'événement. Amazon S3 utilise les versions 2.1, 2.2 et 2.3 de cette structure d'événement. Amazon S3 utilise la version 2.2 pour les notifications d'événements de réplication entre Régions. Il utilise la version 2.3 pour le cycle de vie S3, S3 Intelligent-Tiering, la liste ACL d'objet, le balisage d'objets et les événements de suppression de restauration d'objets. Ces versions contiennent des informations supplémentaires spécifiques à ces opérations. Les versions 2.2 et 2.3 sont par ailleurs compatibles avec la version 2.1, qu'Amazon S3 utilise actuellement pour tous les autres types de notifications d'événements.

```
{
   "Records":[
      {
         "eventVersion":"2.2",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"The time, in ISO-8601 format, for example,
 1970-01-01T00:00:00.000Z, when Amazon S3 finished processing the request",
         "eventName":"event-type",
```

```
         "userIdentity":{
            "principalId":"Amazon-customer-ID-of-the-user-who-caused-the-event"
         },
         "requestParameters":{
            "sourceIPAddress":"ip-address-where-request-came-from"
         },
         "responseElements":{
            "x-amz-request-id":"Amazon S3 generated request ID",
            "x-amz-id-2":"Amazon S3 host that processed the request"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"ID found in the bucket notification configuration",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"Amazon-customer-ID-of-the-bucket-owner"
               },
               "arn":"bucket-ARN"
            },
            "object":{
               "key":"object-key",
               "size":"object-size in bytes",
               "eTag":"object eTag",
               "versionId":"object version if bucket is versioning-enabled, otherwise
 null",
               "sequencer": "a string representation of a hexadecimal value used to
 determine event sequence, only used with PUTs and DELETEs"
            }
         },
         "glacierEventData": {
            "restoreEventData": {
               "lifecycleRestorationExpiryTime": "The time, in ISO-8601 format, for
 example, 1970-01-01T00:00:00.000Z, of Restore Expiry",
               "lifecycleRestoreStorageClass": "Source storage class for restore"
            }
         }
      }
   ]
}
```

Notez les éléments suivants à propos de la structure des messages d'événement :

- La valeur de clé `eventVersion` contient une version majeure et une version mineure au format `<major>.<minor>`.

  La version majeure est incrémentée si Amazon S3 apporte à la structure de l'événement une modification qui n'est pas rétrocompatible. Cela inclut la suppression d'un champ JSON déjà présent ou la modification de la représentation du contenu d'un champ (par exemple, un format de date).

  La version mineure est incrémentée si Amazon S3 ajoute de nouveaux champs à la structure de l'événement. Cela peut se produire si de nouvelles informations sont fournies pour certains ou tous les événements existants. Cela peut également se produire si de nouvelles informations sont fournies sur les types d'événements nouvellement introduits. Les applications doivent ignorer les nouveaux champs pour être compatibles avec de nouvelles versions mineures de la structure de l'événement.

  Si de nouveaux types d'événement sont introduits mais que la structure de l'événement n'est pas modifiée, la version de l'événement ne change pas.

  Pour vous assurer que vos applications puissent analyser correctement la structure de l'événement, nous vous recommandons d'effectuer une comparaison égal à sur le numéro de version majeure. Pour vous assurer que les champs attendus par votre application sont présents, nous vous recommandons également d'effectuer une comparaison greater-than-or-equal -to sur la version mineure.
- Le `eventName` fait référence à la liste des types de notifications d'événements, mais ne contient pas le préfixe `s3:`.
- La valeur `responseElements` clé est utile si vous souhaitez suivre une demande en effectuant un suivi avec AWS Support. Les deux éléments `x-amz-request-id` et `x-amz-id-2` aident Amazon S3 à suivre une demande individuelle. Ces valeurs sont identiques à celles renvoyées par Amazon S3 dans la réponse à la demande qui initie les événements. Ainsi, ils peuvent être utilisés pour faire correspondre l'événement à la demande.
- La clé `s3` fournit les informations relatives à l'objet et au compartiment concernés par l'événement. La valeur du nom de clé d'objet est codée en URL. Par exemple, « fleur rouge.jpg » devient « fleur +rouge.jpg » (Amazon S3 renvoie « `application/x-www-form-urlencoded` » comme type de contenu dans la réponse).
- La clé `sequencer` permet de déterminer la séquence des événements. Les notifications d'événements n'arrivent pas nécessairement dans le même ordre dans lequel les événement se sont produits. Toutefois, les notifications provenant d'événements qui créent des objets (PUTs) et

supprimer des objets qui contiennent un `sequencer`. Il peut être utilisé pour déterminer l'ordre dans lequel se sont produits les événements pour une clé d'objet donnée.

Si vous comparez les chaînes `sequencer` provenant de deux notifications d'événements associées à la même clé d'objet, la notification d'événement qui présente la plus grande valeur `sequencer` hexadécimale correspond à l'événement le plus récent. Si vous utilisez des notifications d'événement pour gérer une base de données ou un index distincts de vos objets Amazon S3, nous vous recommandons de comparer et de stocker les valeurs `sequencer` à mesure que vous traitez les notifications associées à chaque événement.

Remarques :

- Vous ne pouvez pas utiliser `sequencer` pour déterminer l'ordre des événements associés à différentes clés d'objet.
- La longueur des valeurs de séquenceur est variable. Pour comparer ces valeurs, complétez d'abord à droite la valeur la plus courte à l'aide de zéros, puis effectuer une comparaison lexicographique.

- Seule la clé `glacierEventData` est visible pour les événements `s3:ObjectRestore:Completed`.
- La clé `restoreEventData` contient des attributs qui sont liés à votre demande de restauration.
- La clé `replicationEventData` n'est visible que pour les événements de réplication.
- La clé `intelligentTieringEventData` n'est visible que pour les événements S3 Intelligent-Tiering.
- La clé `lifecycleEventData` n'est visible que pour les événements de transition du cycle de vie S3.

Exemples de messages

Voici des exemples de messages de notification d'événement Amazon S3.

Message de test Amazon S3

Une fois que vous avez configuré une notification d'événement pour un compartiment, Amazon S3 envoie le message de test suivant.

```
{
   "Service":"Amazon S3",
   "Event":"s3:TestEvent",
```

```
   "Time":"2014-10-13T15:57:02.089Z",
   "Bucket":"amzn-s3-demo-bucket",
   "RequestId":"5582815E1AEA5ADF",
   "HostId":"8cLeGAmw098X5cv4Zkwcmo8vvZa3eH3eKxsPzbB9wrR+YstdA6Knx4Ip8EXAMPLE"
}
```

> **Note**
>
> Le `s3:TestEvent` message utilise un format différent de celui des notifications d'événements S3 classiques. Contrairement aux autres notifications d'événements qui utilisent la structure `Records` matricielle illustrée ci-dessus, l'événement de test utilise un format simplifié avec des champs directs. Lorsque vous implémentez la gestion des événements, assurez-vous que votre code peut distinguer et gérer correctement les deux formats de message.

Exemple de message envoyé lorsqu'un objet est créé à l'aide d'une requête PUT

Le message suivant est un exemple de message envoyé par Amazon S3 pour publier un événement `s3:ObjectCreated:Put`.

```
{
   "Records":[
      {
         "eventVersion":"2.1",
         "eventSource":"aws:s3",
         "awsRegion":"us-west-2",
         "eventTime":"1970-01-01T00:00:00.000Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"AIDAJDPLRKLG7UEXAMPLE"
         },
         "requestParameters":{
            "sourceIPAddress":"127.0.0.1"
         },
         "responseElements":{
            "x-amz-request-id":"C3D13FE58DE4C810",
            "x-amz-id-2":"FMyUVURIY8/IgAtTv8xRjskZQpcIZ9KG4V5Wp6S7S/
JRWeUWerMUE5JgHvANOjpD"
         },
         "s3":{
```

```
            "s3SchemaVersion":"1.0",
            "configurationId":"testConfigRule",
            "bucket":{
               "name":"amzn-s3-demo-bucket",
               "ownerIdentity":{
                  "principalId":"A3NL1KOZZKExample"
               },
               "arn":"arn:aws:s3:::amzn-s3-demo-bucket"
            },
            "object":{
               "key":"HappyFace.jpg",
               "size":1024,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "versionId":"096fKKXTRTtl3on89fVO.nfljtsv6qko",
               "sequencer":"0055AED6DCD90281E5"
            }
         }
      }
   ]
}
```

Pour connaître la définition de chaque préfixe d'identification IAM (par exemple AIDA, AROA, AGPA), consultez Identifiants IAM dans le Guide de l'utilisateur IAM.

En utilisant EventBridge

Amazon S3 peut envoyer des événements à Amazon EventBridge chaque fois que certains événements se produisent dans votre compartiment. Contrairement à d'autres destinations, vous n'avez pas besoin de sélectionner les types d'événements que vous souhaitez proposer. Une fois EventBridge activé, tous les événements ci-dessous sont envoyés à EventBridge. Vous pouvez utiliser des EventBridge règles pour acheminer les événements vers des cibles supplémentaires. La liste suivante répertorie les événements auxquels Amazon S3 est envoyé EventBridge.

Type d'événement	Description
Objet créé	Un objet a été créé. Le champ Reason de la structure du message d'événement indique quelle API S3 a été utilisée pour créer l'objet : PutObject, POST Object CopyObject, ou CompleteMultipartUpload.

Type d'événement	Description
Objet supprimé (DeleteObject) Objet supprimé (expiration du cycle de vie)	Un objet a été supprimé. Lorsqu'un objet est supprimé à l'aide d'un appel d'API S3, le champ motif est défini sur DeleteObject. Lorsqu'un objet est supprimé par une règle d'expiration du cycle de vie S3, le champ motif est défini sur Expiration du cycle de vie. Pour plus d'informations, consultez Objets en cours d'expiration. Lorsqu'un objet non versionné est supprimé ou lorsqu'un objet versionné est supprimé définitivement, le champ de type de suppression est défini sur Supprimé définitivement. Lorsqu'un marqueur de suppression est créé pour un objet versionné, le champ de type de suppression est défini sur Supprimer le marqueur créé. Pour plus d'informations, consultez Suppression des versions d'objet d'un compartiment activé pour la gestion des versions.
Restauration d'un objet démarrée	Une restauration d'objets a été initiée à partir de la classe de stockage S3 Glacier ou S3 Glacier Deep Archive ou depuis le niveau S3 Intelligent-Tiering Archive Access ou Deep Archive Access. Pour plus d'informations, consultez Utilisation des objets archivés.
Restauration d'un objet terminée	Une restauration d'objets a été terminée.
Restauration d'un objet expiré	La copie temporaire d'un objet restauré à partir de S3 Glacier ou S3 Glacier Deep Archive a expiré et a été supprimée.
Classe de stockage d'objets modifiée	Un objet a été transféré vers une classe de stockage différente. Pour plus d'informations, consultez Transition des objets à l'aide du cycle de vie Amazon S3.

Type d'événement	Description
Niveau d'accès aux objets modifié	Un objet a été transféré vers le niveau S3 Intelligent-Tierin g Archive Access ou Deep Archive Access. Pour plus d'informations, consultez Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering.
Liste ACL d'un objet mise à jour	La liste de contrôle d'accès (ACL) d'un objet a été définie à l'aide de l' PutObjectACL. Un événement n'est pas généré lorsqu'une demande n'entraîne aucune modification de la liste ACL d'un objet. Pour plus d'informations, consultez Présentation de la liste de contrôle d'accès (ACL).
Balises d'objets ajoutées	Un ensemble de balises a été ajouté à un objet à l'aide de PutObjectTagging. Pour de plus amples informations, veuillez consulter Catégorisation de vos objets à l'aide de balises.
Balises d'objets supprimées	Toutes les balises ont été supprimées d'un objet à l'aide de DeleteObjectTagging. Pour de plus amples informations, veuillez consulter Catégorisation de vos objets à l'aide de balises.

> **Note**
>
> Pour plus d'informations sur la façon dont les types d'événements Amazon S3 sont mappés aux types d' EventBridge événements, consultez EventBridge Cartographie et résolution des problèmes sur Amazon.

Vous pouvez utiliser les notifications d'événements Amazon S3 EventBridge pour écrire des règles qui prennent des mesures lorsqu'un événement se produit dans votre compartiment. Par exemple, vous pouvez faire en sorte qu'il vous envoie une notification. Pour plus d'informations, consultez le contenu EventBridge du guide de EventBridge l'utilisateur Amazon.

Pour plus d'informations sur les actions et les types de données avec lesquels vous pouvez interagir à l'aide de l' EventBridge API, consultez la référence d' EventBridge API Amazon dans la référence EventBridge d'API Amazon.

Pour plus d'informations sur les tarifs, consultez EventBridge les tarifs Amazon.

Rubriques

- EventBridge Autorisations Amazon
- Activation d'Amazon EventBridge
- EventBridge structure du message d'événement
- EventBridge Cartographie et résolution des problèmes sur Amazon

EventBridge Autorisations Amazon

Amazon S3 n'a pas besoin d'autorisations supplémentaires pour transmettre des événements à Amazon EventBridge.

Activation d'Amazon EventBridge

Vous pouvez activer Amazon EventBridge à l'aide de la console S3 AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3.

> **Note**
>
> Après l'activation EventBridge, il faut environ cinq minutes pour que les modifications prennent effet.

Utilisation de la console S3

Pour activer la diffusion d' EventBridge événements dans la console S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer les événements.
4. Choisissez Propriétés.

5. Accédez à la section Notifications d'événements et recherchez la EventBridge sous-section Amazon. Choisissez Modifier.
6. Sous Envoyer des notifications à Amazon EventBridge pour tous les événements de ce compartiment, sélectionnez Activé.

À l'aide du AWS CLI

L'exemple suivant crée une configuration de notification de compartiment pour un compartiment sur `amzn-s3-demo-bucket1` lequel Amazon EventBridge est activé.

```
aws s3api put-bucket-notification-configuration --bucket amzn-s3-demo-bucket1 --
notification-configuration='{ "EventBridgeConfiguration": {} }'
```

Utilisation de l'API REST

Vous pouvez activer Amazon par programmation EventBridge sur un bucket en appelant l'API REST Amazon S3. Pour plus d'informations, consultez le PutBucketNotificationConfigurationmanuel Amazon Simple Storage Service API Reference.

L'exemple suivant montre le code XML utilisé pour créer une configuration de notification de compartiment avec Amazon EventBridge activé.

```
<NotificationConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <EventBridgeConfiguration>
  </EventBridgeConfiguration>
</NotificationConfiguration>
```

Création de EventBridge règles

Une fois activé, vous pouvez créer des EventBridge règles Amazon pour certaines tâches. Par exemple, vous pouvez envoyer des notifications par e-mail lorsqu'un objet est créé. Pour un didacticiel complet, consultez Tutoriel : Envoyer une notification lors de la création d'un objet Amazon S3 dans le guide de EventBridge l'utilisateur Amazon.

EventBridge structure du message d'événement

Le message de notification qu'envoie Amazon S3 pour publier un événement est au format JSON. Lorsqu'Amazon S3 envoie un événement à Amazon EventBridge, les champs suivants sont présents.

- version – Actuellement 0 (zéro) pour tous les événements.

- id – UUID généré pour chaque événement.
- detail-type – Type d'événement qui est envoyé. Consultez En utilisant EventBridge pour obtenir la liste des types d'événements.
- source – Identifie le service à l'origine de l'événement.
- account (compte) – ID de Compte AWS à 12 chiffres du propriétaire du compartiment.
- time (heure) – Heure à laquelle l'événement s'est produit.
- region (Région) – Identifie la Région AWS du compartiment.
- resources (ressources) – Tableau JSON contenant l'Amazon Resource Name (ARN) du compartiment.
- detail (détail) – Un objet JSON qui contient les informations sur l'événement. Pour plus d'informations sur ce qui peut être inclus dans ce champ, consultez Champ de détail des messages d'événement.

Exemples de structure de messages d'événements

Vous trouverez ci-dessous des exemples de messages de notification d'événements Amazon S3 qui peuvent être envoyés à Amazon EventBridge.

Objet créé

```
{
  "version": "0",
  "id": "17793124-05d4-b198-2fde-7ededc63b103",
  "detail-type": "Object Created",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
```

```
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "IYV3p45BT0ac8hjHg1houSdS1a.Mro8e",
      "sequencer": "617f08299329d189"
    },
    "request-id": "N4N7GDK58NMKJ12R",
    "requester": "123456789012",
    "source-ip-address": "1.2.3.4",
    "reason": "PutObject"
  }
}
```

Objet supprimé (en utilisant DeleteObject)

```
{
  "version": "0",
  "id": "2ee9cc15-d022-99ea-1fb8-1b1bac4850f9",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "1QW9g1Z99LUNbvaaYVpW9xDlOLU.qxgF",
      "sequencer": "617f0837b476e463"
    },
    "request-id": "0BH729840619AG5K",
    "requester": "123456789012",
    "source-ip-address": "1.2.3.4",
    "reason": "DeleteObject",
    "deletion-type": "Delete Marker Created"
  }
}
```

Objet supprimé (à l'aide de l'expiration du cycle de vie)


```
{
  "version": "0",
  "id": "ad1de317-e409-eba2-9552-30113f8d88e3",
  "detail-type": "Object Deleted",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "etag": "d41d8cd98f00b204e9800998ecf8427e",
      "version-id": "mtB0cV.jejK63XkRNceanNMC.qXPWLeK",
      "sequencer": "617b398000000000"
    },
    "request-id": "20EB74C14654DC47",
    "requester": "s3.amazonaws.com",
    "reason": "Lifecycle Expiration",
    "deletion-type": "Delete Marker Created"
  }
}
```


Restauration d'un objet terminée


```
{
  "version": "0",
  "id": "6924de0d-13e2-6bbf-c0c1-b903b753565e",
  "detail-type": "Object Restore Completed",
  "source": "aws.s3",
  "account": "111122223333",
  "time": "2021-11-12T00:00:00Z",
```

```
  "region": "ca-central-1",
  "resources": [
    "arn:aws:s3:::amzn-s3-demo-bucket1"
  ],
  "detail": {
    "version": "0",
    "bucket": {
      "name": "amzn-s3-demo-bucket1"
    },
    "object": {
      "key": "example-key",
      "size": 5,
      "etag": "b1946ac92492d2347c6235b4d2611184",
      "version-id": "KKsjUC1.6gIjqtvhfg5AdMI0eCePIiT3"
    },
    "request-id": "189F19CB7FB1B6A4",
    "requester": "s3.amazonaws.com",
    "restore-expiry-time": "2021-11-13T00:00:00Z",
    "source-storage-class": "GLACIER"
  }
}
```

Champ de détail des messages d'événement

Le champ de détails contient un objet JSON avec des informations sur l'événement. Les champs suivants peuvent être présents dans le champ de détail.

- version – Actuellement 0 (zéro) pour tous les événements.
- bucket (compartiment) – Informations relatives au compartiment Amazon S3 impliqué dans l'événement.
- object (objet) – Informations relatives à l'objet Amazon S3 impliqué dans l'événement.
- request-id – ID de demande dans la réponse S3.
- demandeur — Compte AWS ID ou principal AWS de service du demandeur.
- source-ip-address— Adresse IP source de la requête S3. Présent uniquement pour les événements déclenchés par une demande S3.
- reason — Pour les événements Object Created, l'API S3 utilisée pour créer l'objet : PutObject, POST Object CopyObject, ou CompleteMultipartUpload. Pour les événements Object Deleted, ce paramètre est défini sur DeleteObjectlorsqu'un objet est supprimé par un appel d'API S3, ou sur

Expiration du cycle de vie lorsqu'un objet est supprimé par une règle d'expiration du cycle de vie S3. Pour de plus amples informations, veuillez consulter Objets en cours d'expiration.

- deletion-type – Pour les événements Objet supprimé, lorsqu'un objet non versionné est supprimé ou lorsqu'un objet versionné est supprimé définitivement, ce champ est défini sur Supprimé définitivement. Lorsqu'un marqueur de suppression est créé pour un objet versionné, ce champ est défini sur Supprimer le marqueur créé. Pour de plus amples informations, veuillez consulter Suppression des versions d'objet d'un compartiment activé pour la gestion des versions.

> **Note**
>
> Certains attributs d'objet (comme `etag` et `size`) ne sont présents que lorsqu'un marqueur de suppression est créé.

- restore-expiry-time— Pour les événements Object Restore Completed, heure à laquelle la copie temporaire de l'objet sera supprimée de S3. Pour de plus amples informations, veuillez consulter Utilisation des objets archivés.
- source-storage-class— Pour les événements Object Restore Initiated et Object Restore Completed, classe de stockage de l'objet en cours de restauration. Pour de plus amples informations, veuillez consulter Utilisation des objets archivés.
- destination-storage-class— Pour les événements Object Storage Class Changed, nouvelle classe de stockage de l'objet. Pour de plus amples informations, veuillez consulter Transition des objets à l'aide du cycle de vie Amazon S3.
- destination-access-tier— Pour les événements Object Access Tier Changed, nouveau niveau d'accès de l'objet. Pour de plus amples informations, veuillez consulter Gestion des coûts de stockage avec Amazon S3 Intelligent-Tiering.

EventBridge Cartographie et résolution des problèmes sur Amazon

Le tableau suivant décrit comment les types d'événements Amazon S3 sont mappés aux types d' EventBridge événements Amazon.

Type d'événement S3	Type de EventBridge détail Amazon
ObjectCreated:Mettre ObjectCreated:Publier	Objet créé

Type d'événement S3	Type de EventBridge détail Amazon
ObjectCreated:Copier ObjectCreated:CompleteMultipartUpload	
ObjectRemoved:Supprimer ObjectRemoved:DeleteMarkerCreated LifecycleExpiration:Supprimer LifecycleExpiration:DeleteMarkerCreated	Objet supprimé
ObjectRestore:Publier	Restauration d'un objet démarrée
ObjectRestore:Terminé	Restauration d'un objet terminée
ObjectRestore:Supprimer	Restauration d'un objet expiré
LifecycleTransition	Classe de stockage d'objets modifiée
IntelligentTiering	Niveau d'accès aux objets modifié
ObjectTagging:Mettre	Balises d'objets ajoutées
ObjectTagging:Supprimer	Balises d'objets supprimées
ObjectAcl:Mettre	Liste ACL d'un objet mise à jour

EventBridge Résolution des problèmes liés à Amazon

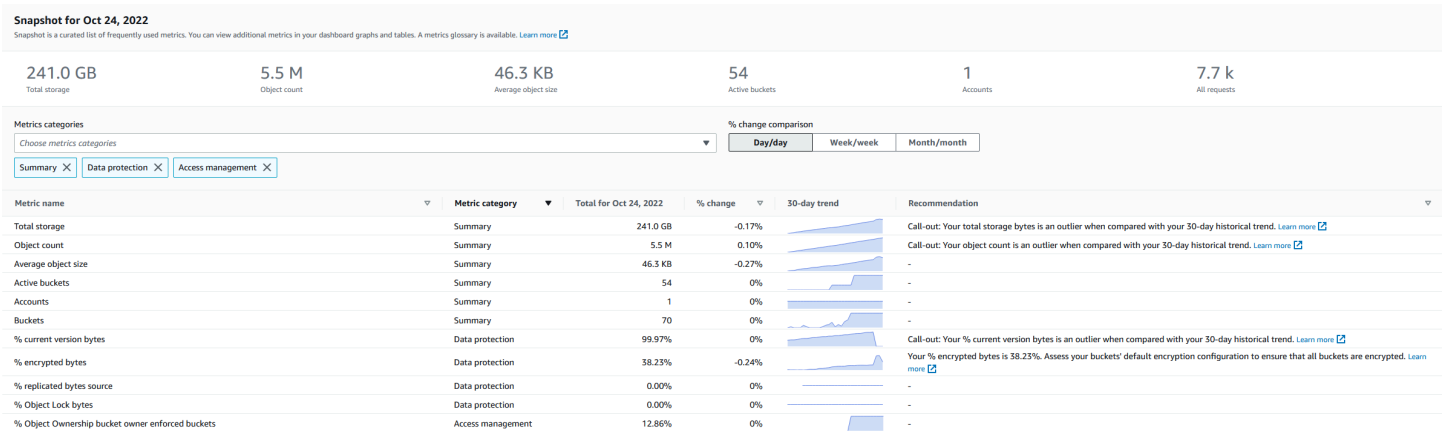
Pour plus d'informations sur le dépannage EventBridge, consultez la section Résolution des problèmes liés EventBridge à Amazon dans le guide de EventBridge l'utilisateur Amazon.

Évaluer l'activité et l'utilisation de votre stockage avec Amazon S3 Storage Lens

Amazon S3 Storage Lens est une fonctionnalité d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur le stockage et l'activité des objets. S3 Storage Lens analyse également les métriques de stockage pour fournir des recommandations contextuelles afin d'aider à réduire les coûts de stockage et à appliquer les bonnes pratiques de protection des données.

Vous pouvez utiliser les métriques S3 Storage Lens pour générer des informations récapitulatives. Par exemple, vous pouvez connaître la quantité de stockage dont vous disposez dans l'ensemble de votre organisation ou les compartiments et préfixes dont la croissance est la plus rapide. Vous pouvez également utiliser les métriques S3 Storage Lens pour identifier des opportunités d'optimisation des coûts, mettre en œuvre les bonnes pratiques de protection des données et de gestion des accès, et améliorer les performances des charges de travail d'application. Par exemple, vous pouvez identifier les buckets pour lesquels les règles du cycle de vie S3 ne sont pas configurées pour faire expirer les téléchargements partitionnés incomplets datant de plus de 7 jours. Vous pouvez également identifier les compartiments qui ne respectent pas les bonnes pratiques de protection des données, telles que l'utilisation de la réplication S3 ou de la gestion des versions S3.

S3 Storage Lens regroupe vos métriques et affiche les informations dans la section Account snapshot (Instantané du compte) sur la page Buckets (Compartiments) de la console Amazon S3. S3 Storage Lens fournit également un tableau de bord interactif que vous pouvez utiliser pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord dispose d'options d'exploration pour générer et visualiser des informations au niveau de l'organisation, du compte, de la Région AWS, de la classe de stockage, du compartiment, du préfixe ou du groupe Storage Lens. Vous pouvez également envoyer une exportation de métriques quotidienne au format CSV ou Parquet vers un compartiment S3.



Métriques et fonctionnalités S3 Storage Lens

S3 Storage Lens fournit un tableau de bord par défaut interactif qui est mis à jour quotidiennement. S3 Storage Lens préconfigure ce tableau de bord pour qu'il affiche le résumé des informations et des tendances pour l'ensemble de votre compte, et les met à jour quotidiennement dans la console S3. Les métriques de ce tableau de bord sont également résumées dans l'instantané du compte sur la page Buckets (compartiments). Pour de plus amples informations, veuillez consulter Tableau de bord par défaut.

Pour créer d'autres tableaux de bord et les définir en fonction Régions AWS de compartiments ou de comptes S3 (pour AWS Organizations), vous devez créer une configuration de tableau de bord S3 Storage Lens. Vous pouvez créer et gérer les configurations du tableau de bord S3 Storage Lens à l'aide de la console Amazon S3 AWS SDKs, AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. Lorsque vous créez ou modifiez un tableau de bord S3 Storage Lens, vous définissez la portée de ce tableau de bord et la sélection des métriques.

S3 Storage Lens fournit des métriques et des recommandations avancées, que vous pouvez utiliser moyennant des frais supplémentaires. Les métriques et recommandations avancées vous donnent accès à des métriques et à des fonctionnalités supplémentaires pour mieux comprendre votre stockage. Ces fonctionnalités incluent les catégories de métriques avancées, l'agrégation de préfixes, les recommandations contextuelles et la publication sur Amazon CloudWatch. L'agrégation de préfixes et les recommandations contextuelles sont disponibles uniquement dans la console Amazon S3. Pour obtenir des informations sur la tarification de S3 Storage Lens, consultez la tarification Amazon S3.

Catégories de métriques

Aux niveaux gratuit et avancé, les métriques sont organisées en catégories correspondant aux principaux cas d'utilisation, tels que l'optimisation des coûts et la protection des données. Les

métriques gratuites incluent le résumé, l'optimisation des coûts, la protection des données, la gestion des accès, les performances et les métriques d'événements. Lorsque vous passez à des métriques et à des recommandations avancées, vous pouvez activer des métriques avancées sur l'optimisation des coûts et la protection des données. Vous pouvez utiliser ces métriques avancées pour réduire encore vos coûts de stockage S3 et améliorer votre position en matière de protection des données. Vous pouvez également activer les métriques d'activité et les métriques de codes de statut détaillés afin d'améliorer les performances des charges de travail d'application qui accèdent à vos compartiments S3. Pour plus d'informations sur les catégories des métriques gratuites et avancées, consultez Sélection des métriques.

Vous pouvez évaluer votre stockage en fonction des bonnes pratiques dans S3, telles que l'analyse du pourcentage de compartiments pour lesquels le chiffrement, le verrouillage d'objets S3 ou la gestion des versions S3 sont activés. Vous pouvez également identifier les opportunités d'économies potentielles. Par exemple, vous pouvez utiliser des métriques relatives aux nombres de règles de cycle de vie S3 pour identifier les compartiments auxquels il manque des règles de cycle de vie d'expiration ou de transition. Vous pouvez également identifier analyser votre activité de demandes par compartiment afin de trouver des compartiments dont les objets pourraient être transférés vers une classe de stockage moins coûteuse. Pour de plus amples informations, veuillez consulter Cas d'utilisation des métriques Amazon S3 Storage Lens.

Exportation de métriques

Outre la visualisation du tableau de bord dans la console S3, vous pouvez exporter les métriques au format CSV ou Parquet vers un compartiment S3 pour une analyse approfondie avec l'outil d'analytique de votre choix. Pour de plus amples informations, veuillez consulter Afficher les métriques Amazon S3 Storage Lens à l'aide d'une exportation de données.

CloudWatch Publication sur Amazon

Vous pouvez publier les statistiques d'utilisation et d'activité de S3 Storage Lens sur Amazon CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatch tableaux de bord. Vous pouvez également utiliser des CloudWatch fonctionnalités, telles que les alarmes et les actions déclenchées, les mathématiques métriques et la détection des anomalies, pour surveiller et agir sur les métriques S3 Storage Lens. En outre, les opérations CloudWatch d'API permettent aux applications, y compris aux fournisseurs tiers, d'accéder à vos métriques S3 Storage Lens. L'option de CloudWatch publication est disponible pour les tableaux de bord mis à niveau vers les métriques et recommandations avancées de S3 Storage Lens. Pour plus d'informations sur la prise en charge des métriques S3 Storage Lens dans CloudWatch, consultezSurveillez les métriques de S3 Storage Lens dans CloudWatch.

Pour plus d'informations sur l'utilisation de S3 Storage Lens, consultez les rubriques suivantes.

Rubriques

- Présentation d'Amazon S3 Storage Lens
- Glossaire des métriques Amazon S3 Storage Lens
- Définition d'autorisations Amazon S3 Storage Lens
- Utilisation d'Amazon S3 Storage Lens à l'aide de la console et de l'API
- Affichage des métriques avec Amazon S3 Storage Lens
- Utilisation d'Amazon S3 Storage Lens avec AWS Organizations
- Utilisation des groupes S3 Storage Lens pour filtrer et agréger des métriques

Présentation d'Amazon S3 Storage Lens

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Amazon S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Vous pouvez utiliser les métriques S3 Storage Lens pour générer des informations récapitulatives, telles que la quantité de stockage dont vous disposez dans l'ensemble de votre organisation ou les compartiments et préfixes qui connaissent la croissance la plus rapide. Vous pouvez également utiliser les métriques S3 Storage Lens pour identifier les opportunités d'optimisation des coûts, mettre en œuvre les bonnes pratiques de protection et de sécurisation des données et améliorer les performances des charges de travail d'application. Par exemple, vous

pouvez identifier les compartiments qui sont dépourvus de règles de cycle de vie S3 pour faire expirer les chargements partitionnés non terminés datant de plus de 7 jours. Vous pouvez également identifier les compartiments qui ne respectent pas les bonnes pratiques de protection des données, telles que l'utilisation de la réplication S3 ou de la gestion des versions S3. S3 Storage Lens analyse également les métriques de stockage pour fournir des recommandations contextuelles afin d'aider à réduire les coûts de stockage et à appliquer les bonnes pratiques de protection des données.

S3 Storage Lens regroupe vos métriques et affiche les informations dans la section Account snapshot (Instantané du compte) sur la page Buckets (Compartiments) de la console Amazon S3. S3 Storage Lens fournit également un tableau de bord interactif que vous pouvez utiliser pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord dispose d'options d'exploration pour générer et visualiser des informations au niveau de l'organisation, du compte, de la Région AWS, de la classe de stockage, du compartiment, du préfixe ou du groupe Storage Lens. Vous pouvez également envoyer une exportation de métriques quotidienne au format CSV ou Parquet vers un compartiment S3. Vous pouvez créer et gérer des tableaux de bord S3 Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) ou de l'API REST Amazon S3. AWS SDKs

Concepts et terminologie propres à S3 Storage Lens

Cette section contient la terminologie et les concepts essentiels pour bien comprendre et utiliser Amazon S3 Storage Lens.

Rubriques

- Configuration du tableau de bord
- Tableau de bord par défaut
- Tableaux de bord
- Instantané du compte
- Exportation de métriques
- Région d'accueil
- Période de conservation
- Catégories de métriques
- Recommandations
- Sélection des métriques

- Lentille de stockage S3 et AWS Organizations

Configuration du tableau de bord

S3 Storage Lens nécessite une configuration de tableau de bord contenant les propriétés requises pour agréger les métriques en votre nom pour un seul tableau de bord ou une seule exportation. Lorsque vous créez une configuration, vous choisissez le nom du tableau de bord et la région d'origine, que vous ne pouvez pas modifier après avoir créé le tableau de bord. Vous pouvez éventuellement ajouter des étiquettes et configurer une exportation des métriques au format CSV ou Parquet.

Dans la configuration du tableau de bord, vous définissez également la portée du tableau de bord et la sélection des métriques. La portée peut inclure tout le stockage du compte de votre organisation ou des sections filtrées par région, compartiment et compte. Lorsque vous configurez la sélection de métriques, vous pouvez choisir entre des métriques gratuites et des métriques et recommandations avancées, que vous pouvez utiliser moyennant des frais supplémentaires. Les métriques et recommandations avancées vous donnent accès à des métriques et à des fonctionnalités supplémentaires. Ces fonctionnalités incluent les catégories de mesures avancées, l'agrégation au niveau des préfixes, les recommandations contextuelles et la publication sur Amazon. CloudWatch Pour obtenir des informations sur la tarification de S3 Storage Lens, consultez la tarification Amazon S3.

Tableau de bord par défaut

Le tableau de bord par défaut de S3 Storage Lens sur la console est nommé default-account-dashboard. S3 préconfigure ce tableau de bord pour qu'il affiche le résumé des informations et des tendances pour l'ensemble de votre compte, et les met à jour quotidiennement dans la console S3. Vous ne pouvez pas modifier la portée de la configuration du tableau de bord par défaut, mais vous pouvez mettre à niveau la sélection des métriques en passant des métriques gratuites aux métriques et recommandations avancées. Vous pouvez configurer l'exportation facultative des métriques ou même désactiver le tableau de bord. Toutefois, vous ne pouvez pas supprimer le tableau de bord par défaut.

> **Note**
>
> Si vous désactivez le tableau de bord par défaut, il n'est plus mis à jour. Vous ne recevrez plus de nouvelles métriques quotidiennes dans votre tableau de bord S3 Storage Lens, votre exportation de métriques ou l'instantané de compte sur la page S3 Compartiments. Si votre

tableau de bord utilise des indicateurs et des recommandations avancés, vous ne serez plus facturé. Vous pourrez toujours voir les données d'historique dans le tableau de bord jusqu'à l'expiration du délai de 14 jours pour les requêtes de données. Cette période est de 15 mois si vous avez activé les métriques et recommandations avancées. Pour accéder aux données d'historique, vous pouvez réactiver le tableau de bord pendant la période d'expiration.

Tableaux de bord

Vous pouvez créer des tableaux de bord S3 Storage Lens supplémentaires et les définir en Régions AWS fonction de compartiments S3 ou de comptes (pour AWS Organizations). Lorsque vous créez ou modifiez un tableau de bord S3 Storage Lens, vous définissez la portée de ce tableau de bord et la sélection des métriques. S3 Storage Lens fournit des métriques et des recommandations avancées, que vous pouvez utiliser moyennant des frais supplémentaires. Les métriques et recommandations avancées vous donnent accès à des métriques et à des fonctionnalités supplémentaires pour mieux comprendre votre stockage. Il s'agit notamment des catégories de mesures avancées, de l'agrégation au niveau des préfixes, des recommandations contextuelles et de la publication sur Amazon. CloudWatch Pour obtenir des informations sur la tarification de S3 Storage Lens, consultez la tarification Amazon S3.

Vous pouvez également désactiver ou supprimer les tableaux de bord. Si vous désactivez un tableau de bord, il ne sera plus mis à jour et vous ne recevrez plus de nouvelles métriques quotidiennes. Vous pouvez encore voir les données d'historique pendant la période d'expiration de 14 jours. Si vous avez activé les métriques et recommandations avancées pour ce tableau de bord, cette période est de 15 mois. Pour accéder aux données d'historique, vous pouvez réactiver le tableau de bord pendant la période d'expiration.

Si vous supprimez votre tableau de bord, vous perdrez tous ses paramètres de configuration. Vous ne recevrez plus de nouvelles métriques quotidiennes et vous perdrez également l'accès aux données historiques associées à ce tableau de bord. Si vous souhaitez accéder aux données historiques d'un tableau de bord supprimé, vous devez créer un autre tableau de bord portant le même nom dans la même Région d'accueil.

Note

- Vous pouvez utiliser S3 Storage Lens pour créer jusqu'à 50 tableaux de bord par Région d'accueil.

- Les tableaux de bord au niveau de l'organisation ne peuvent être limités qu'à une portée régionale.

Instantané du compte

La fonctionnalité S3 Storage Lens Account snapshot (Instantané du compte) résume les métriques de votre tableau de bord par défaut et affiche votre stockage total, le nombre d'objets et la taille d'objet moyenne sur la page Buckets (compartiments) de la console S3. Cet instantané de compte vous permet d'accéder rapidement aux informations sur le stockage sans avoir à quitter la page Buckets (Compartiments). L'instantané du compte permet également d'accéder en un clic à votre tableau de bord S3 Storage Lens interactif.

Vous pouvez utiliser votre tableau de bord pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord dispose d'options d'exploration pour générer des informations au niveau de l'organisation, du compte, du compartiment, de l'objet ou du préfixe. Vous pouvez également envoyer une exportation de métriques quotidienne au format CSV ou Parquet vers un compartiment S3.

Vous ne pouvez pas modifier la portée du tableau de bord default-account dashboard (tableau de bord de compte par défaut) car il est lié à Account snapshot (Instantané du compte). Cependant, vous pouvez améliorer la sélection de mesures dans votre sélection, en default-account-dashboardpassant de mesures gratuites à des mesures et recommandations avancées payantes. Après cette mise à niveau, vous pouvez afficher toutes les demandes, les octets chargés et les octets téléchargés dans Account snapshot (Instantané du compte) S3 Storage Lens.

> **Note**
>
> Si vous désactivez votre tableau de bord par défaut, Account snapshot (Instantané du compte) n'est plus mis à jour. Pour continuer à afficher les statistiques dans l'instantané du compte, vous pouvez réactiver le default-account-dashboard.

Exportation de métriques

Une exportation de métriques S3 Storage Lens est un fichier contenant toutes les métriques identifiées dans votre configuration S3 Storage Lens. Ces informations sont générées quotidiennement au format CSV ou Parquet, et envoyées dans un compartiment S3. Vous pouvez

utiliser l'exportation des métriques pour une analyse approfondie à l'aide de l'outil de métriques de votre choix. Le compartiment S3 pour l'exportation de vos métriques doit se trouver dans la même Région que la configuration de votre S3 Storage Lens. Vous pouvez générer une exportation de métriques S3 Storage Lens à partir de la console S3 en modifiant la configuration de votre tableau de bord. Vous pouvez également configurer une exportation de métriques à l'aide des touches AWS CLI et AWS SDKs.

Région d'accueil

La région d'origine est l' Région AWS endroit où sont stockées toutes les métriques S3 Storage Lens pour une configuration de tableau de bord donnée. Vous devez choisir une région d'origine lorsque vous créez votre configuration de tableau de bord S3 Storage Lens. Une fois que vous avez choisi une région d'origine, vous ne pouvez pas la modifier. De plus, si vous créez un groupe Storage Lens, nous vous recommandons de choisir la même région d'origine que celle de votre tableau de bord Storage Lens.

> **Note**
>
> Vous pouvez choisir l'une des régions suivantes comme région d'origine :
>
> - USA Est (Virginie du Nord) – `us-east-1`
> - USA Est (Ohio) – `us-east-2`
> - USA Ouest (Californie du Nord) – `us-west-1`
> - USA Ouest (Oregon) – `us-west-2`
> - Asie-Pacifique (Mumbai) – `ap-south-1`
> - Asie-Pacifique (Séoul) – `ap-northeast-2`
> - Asie-Pacifique (Singapour) – `ap-southeast-1`
> - Asie-Pacifique (Sydney) – `ap-southeast-2`
> - Asie-Pacifique (Tokyo) – `ap-northeast-1`
> - Canada (Centre) – `ca-central-1`
> - Chine (Pékin) – `cn-north-1`
> - Chine (Ningxia) – `cn-northwest-1`
> - Europe (Francfort) – `eu-central-1`
> - Europe (Irlande) – `eu-west-1`
> - Europe (Londres) – `eu-west-2`

- Europe (Paris) – `eu-west-3`
- Europe (Stockholm) – `eu-north-1`
- Amérique du Sud (São Paulo) – `sa-east-1`

Période de conservation

Les métriques S3 Storage Lens sont conservées pour que vous puissiez voir les tendances historiques et comparer les différences de stockage et d'activité au fil du temps. Vous pouvez utiliser les métriques Amazon S3 Storage Lens pour les requêtes, pour observer les tendances historiques et comparer les différences d'utilisation et d'activité du stockage au fil du temps.

Toutes les métriques de S3 Storage Lens sont conservées pour une durée de 15 mois. Toutefois, les métriques ne sont disponibles que pour les requêtes d'une durée spécifique, qui dépend de votre sélection des métriques. Cette durée ne peut pas être modifiée. Pour les requêtes, les métriques gratuites sont disponibles pendant 14 jours et les métriques avancées sont disponibles pendant 15 mois.

Catégories de métriques

Dans les niveaux gratuit et avancé, les métriques S3 Storage Lens sont organisées en catégories correspondant aux principaux cas d'utilisation, tels que l'optimisation des coûts et la protection des données. Les métriques gratuites incluent le résumé, l'optimisation des coûts, la protection des données, la gestion des accès, les performances et les métriques d'événements. Lorsque vous passez à des métriques et à des recommandations avancées, vous pouvez activer des métriques supplémentaires sur l'optimisation des coûts et la protection des données que vous pouvez utiliser pour réduire encore vos coûts de stockage S3 et assurer la protection de vos données. Vous pouvez également activer des métriques d'activité et des métriques de codes de statut détaillés que vous pouvez utiliser pour améliorer les performances des flux de travail des applications.

La liste suivante montre toutes les catégories de métriques gratuites et avancées. Pour obtenir la liste complète des métriques individuelles incluses dans chaque catégorie, consultez le glossaire des métriques.

Métriques de résumé

Les métriques récapitulatives fournissent des informations générales sur votre stockage S3, y compris le nombre total d'octets de stockage et le nombre d'objets.

Métriques sur l'optimisation des coûts

Les métriques sur l'optimisation des coûts fournissent des informations que vous pouvez utiliser pour gérer et optimiser vos coûts de stockage. Par exemple, vous pouvez identifier les compartiments contenant des chargements partitionnés non terminés datant de plus de 7 jours.

Les métriques et recommandations avancées vous permettent d'activer des métriques avancées sur l'optimisation des coûts. Ces métriques incluent les métriques relatives aux nombres de règles de cycle de vie S3 que vous pouvez utiliser pour obtenir les nombres de règles de cycle de vie S3 d'expiration et de transition par compartiment.

Métriques sur la protection des données

Les métriques sur la protection des données fournissent des informations sur les fonctionnalités de protection des données, telles que le chiffrement et la gestion des versions S3. Vous pouvez utiliser ces métriques pour identifier les compartiments qui ne respectent pas les bonnes pratiques de protection des données. Par exemple, vous pouvez identifier les compartiments qui n'utilisent pas le chiffrement par défaut avec AWS Key Management Service clés (SSE-KMS) ou le versionnement S3.

Les métriques et recommandations avancées vous permettent d'activer des métriques avancées sur la protection des données. Ces métriques incluent des métriques relatives aux nombres de règles de réplication par compartiment.

Métriques de gestion des accès

Les métriques de gestion des accès fournissent des informations sur la propriété des objets S3. Vous pouvez utiliser ces métriques pour voir les paramètres de propriété d'objets utilisés par vos compartiments.

Métriques d'événements

Les métriques d'événements fournissent des informations pour les notifications d'événements S3. Les métriques d'événements vous permettent de voir quels compartiments ont des notifications d'événements S3 configurées.

Métriques de performances

Les métriques de performances fournissent des informations pour S3 Transfer Acceleration. Les métriques de performances vous permettent de voir dans quels compartiments l'accélération des transferts est activée.

Métriques d'activité (avancées)

Si vous mettez à niveau votre tableau de bord vers Métriques et recommandations avancées, vous pouvez activer les métriques d'activité. Les métriques d'activité fournissent des informations détaillées sur la façon dont votre stockage est sollicité par demandes (par exemple, Toutes les demandes, Demandes Get, Demandes Put), sur les octets chargés ou téléchargés et sur les erreurs.

Les métriques d'activité au niveau des préfixes vous aident à identifier les préfixes rarement utilisés, afin que vous puissiez passer à une classe de stockage plus optimale à l'aide de S3 Lifecycle.

Métriques de codes de statut détaillées (avancées)

Si vous mettez à niveau votre tableau de bord vers Métriques et recommandations avancées, vous pouvez activer les métriques de codes de statut détaillées. Les métriques de codes de statut détaillées fournissent des informations sur les codes de statut HTTP, tels que 403 Forbidden et 503 Service non disponible, que vous pouvez utiliser pour résoudre les problèmes d'accès ou de performances. Par exemple, vous pouvez consulter la métrique Nombre d'erreurs 403 Forbidden pour identifier les charges de travail qui accèdent à des compartiments sans appliquer les autorisations appropriées.

Les métriques de codes de statut détaillées au niveau des préfixes permettent de mieux comprendre les occurrences des codes de statut HTTP par préfixe. Par exemple, les métriques du nombre d'erreurs 503 vous permettent d'identifier les préfixes qui reçoivent des demandes de limitation lors de l'ingestion de données.

Recommandations

S3 Storage Lens fournit des recommandations automatiques pour vous aider à optimiser votre stockage. Les recommandations sont placées contextuellement à côté des métriques concernées dans le tableau de bord S3 Storage Lens. Les données historiques ne sont pas éligibles aux recommandations, car les recommandations concernent ce qui se passe au cours de la période la plus récente. Les recommandations n'apparaissent que lorsqu'elles sont pertinentes.

Les recommandations de S3 Storage Lens sont présentées sous les formes suivantes :

- Suggestions

  Les suggestions vous alertent sur les tendances de stockage et d'activité pouvant indiquer une possibilité d'optimisation des coûts de stockage ou une bonne pratique de protection des données. Vous pouvez utiliser les rubriques suggérées dans le Guide de l'utilisateur Amazon S3 et le tableau

de bord S3 Storage Lens pour effectuer une exploration permettant d'obtenir plus d'informations sur des régions, des compartiments ou des préfixes.

- Alertes

  Les alertes sont des recommandations qui vous signalent les anomalies intéressantes dans le stockage et l'activité au cours d'une période et qui pourraient nécessiter davantage d'attention ou de surveillance.

  - Alertes d'anomalies

    S3 Storage Lens fournit des alertes pour les métriques qui sont des anomalies, basées sur votre tendance des 30 derniers jours. Les anomalies sont calculées à l'aide d'un score standard, également connu sous le nom de score z. Dans ce score, la métrique du jour est soustraite de la moyenne des 30 derniers jours pour la métrique concernée. La métrique du jour est ensuite divisée par l'écart-type de cette métrique au cours des 30 derniers jours. Le score obtenu est généralement compris entre -3 et +3. Ce nombre représente le nombre d'écarts-types entre la métrique du jour et la moyenne.

    S3 Storage Lens considère les métriques ayant un score **>** 2 ou **<** -2 comme des anomalies, car elles sont supérieures ou inférieures à 95 % des données normalement distribuées.

  - Alertes de changement significatif

    L'alerte de changement significatif s'applique aux métriques qui sont censées changer moins fréquemment. Par conséquent, elle est définie sur une sensibilité plus élevée que le calcul des anomalies, qui se situe généralement dans un intervalle de +/- 20 % par rapport au jour, à la semaine ou au mois précédents.

    Réagir aux alertes liées au stockage et à l'activité : une alerte de changement significatif ne reflète pas nécessairement un problème. Elle peut être le résultat d'un changement prévu de votre stockage. Par exemple, il se peut que vous ayez récemment ajouté ou supprimé un nombre important d'objets ou apporté d'autres modifications planifiées de ce type.

    Si vous voyez une alerte de changement significatif sur votre tableau de bord, prenez-en note et déterminez si elle peut être expliquée par des circonstances récentes. Si ce n'est pas le cas, utilisez le tableau de bord S3 Storage Lens pour effectuer une exploration et obtenir plus de détails afin de comprendre quels Régions, compartiments ou préfixes spécifiques sont à l'origine de la fluctuation.

- Rappels

Les rappels fournissent des informations sur le fonctionnement d'Amazon S3. Ils peuvent vous aider à comprendre comment utiliser les fonctions S3 permettant de réduire les coûts de stockage ou d'appliquer les bonnes pratiques de protection des données.

Sélection des métriques

S3 Storage Lens propose deux sélections de métriques que vous pouvez choisir pour votre tableau de bord et pour l'exportation : des métriques gratuites et des métriques et recommandations avancées.

- Métriques gratuites

  S3 Storage Lens propose des métriques gratuites pour tous les tableaux de bord et configurations. Les métriques gratuites contiennent des métriques pertinentes pour votre stockage, telles que le nombre de compartiments et les objets dans votre compte. Les métriques gratuites incluent également des métriques basées sur des cas d'utilisation (par exemple, les métriques sur l'optimisation des coûts et la protection des données) que vous pouvez utiliser pour vérifier si votre stockage est configuré conformément aux bonnes pratiques dans S3. L'ensemble des métriques gratuites sont collectées quotidiennement. Les données sont disponibles pour les requêtes pendant 14 jours. Pour plus d'informations sur les métriques disponibles avec les métriques gratuites, consultez Glossaire des métriques Amazon S3 Storage Lens.

- Métriques et recommandations avancées

  S3 Storage Lens offre des métriques gratuites pour tous les tableaux de bord et configurations, avec la possibilité d'une mise à niveau vers les métriques et recommandations avancées. Des frais supplémentaires s'appliquent. Pour de plus amples informations, veuillez consulter Tarification Amazon S3.

  Les métriques et recommandations avancées incluent toutes les métriques gratuites et des métriques supplémentaires, telles que les métriques avancées sur la protection des données et l'optimisation des coûts, ainsi que des métriques d'activité et des métriques de codes de statut détaillés. Les métriques et recommandations avancées fournissent également des recommandations pour vous aider à optimiser votre stockage. Les recommandations sont placées contextuellement à côté des métriques concernées dans le tableau de bord.

  Les métriques et recommandations avancées incluent les fonctionnalités suivantes :

- Métriques avancées : générez des métriques supplémentaires. Pour obtenir la liste complète des catégories de métriques avancées, consultez Catégories de métriques. Pour obtenir la liste complète des métriques, consultez Glossaire des métriques Amazon S3 Storage Lens.
- Amazon CloudWatch Publishing — Publie les métriques S3 Storage Lens CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatch tableaux de bord. Vous pouvez également utiliser les opérations et fonctionnalités de CloudWatch l'API, telles que les alarmes et les actions déclenchées, les mathématiques métriques et la détection des anomalies, pour surveiller les métriques S3 Storage Lens et prendre des mesures en conséquence. Pour de plus amples informations, veuillez consulter Surveillez les métriques de S3 Storage Lens dans CloudWatch.
- Regroupement des préfixes : collecte des métriques au niveau du préfixe. L'activation du regroupement des préfixes étend toutes les métriques incluses dans la configuration de votre tableau de bord au niveau du préfixe. Les métriques ne sont générées que pour les préfixes qui atteignent le seuil configuré. Notez que les métriques applicables au niveau du préfixe sont disponibles avec la fonctionnalité Regroupement des préfixes, à l'exception des paramètres au niveau du compartiment et des métriques relatives au nombre de règles. Les métriques au niveau du préfixe ne sont pas publiées sur. CloudWatch
- Regroupement des groupes Storage Lens : collecte des métriques au niveau du groupe Storage Lens. Après avoir activé Métriques et recommandations avancées et Regroupement des groupes Storage Lens, vous pouvez spécifier les groupes Storage Lens à inclure ou à exclure de votre tableau de bord Storage Lens. Vous devez spécifier au moins un groupe Storage Lens. Les groupes Storage Lens spécifiés doivent également résider dans la région d'origine désignée dans le compte du tableau de bord. Les métriques au niveau du groupe Storage Lens ne sont pas publiées sur. CloudWatch

L'ensemble des métriques avancées sont collectées quotidiennement. Les données sont disponibles pour les requêtes jusqu'à 15 mois. Pour plus d'informations sur les métriques de stockage agrégées par S3 Storage Lens, consultez Glossaire des métriques Amazon S3 Storage Lens.

> **Note**
>
> Les recommandations sont disponibles uniquement lorsque vous utilisez le tableau de bord S3 Storage Lens sur la console Amazon S3.

Lentille de stockage S3 et AWS Organizations

AWS Organizations est un outil Service AWS qui vous permet de regrouper l'ensemble de vos organisations Comptes AWS au sein d'une seule hiérarchie. Amazon S3 Storage Lens fonctionne avec AWS Organizations pour fournir une vue unique du stockage d'objets et de l'activité sur votre espace de stockage Amazon S3.

Pour de plus amples informations, veuillez consulter Utilisation d'Amazon S3 Storage Lens avec AWS Organizations.

- Accès sécurisé

  À l'aide du compte de gestion de votre organisation, vous devez activer l'accès sécurisé pour S3 Storage Lens afin d'agréger les métriques de stockage et les données d'utilisation pour tous les comptes membres de votre organisation. Vous pouvez ensuite créer des tableaux de bord ou des exportations pour votre organisation à l'aide de votre compte de gestion ou en accordant un accès administrateur délégué à d'autres comptes de votre organisation.

  Vous pouvez désactiver l'accès sécurisé de S3 Storage Lens à tout moment pour empêcher S3 Storage Lens d'agréger les métriques de votre organisation.
- Administrateur délégué

  Vous pouvez créer des tableaux de bord et des métriques pour S3 Storage Lens pour votre organisation en utilisant votre compte de AWS Organizations gestion ou en accordant un accès administrateur délégué à d'autres comptes de votre organisation. Vous pouvez désinscrire les administrateurs délégués à tout moment. La désinscription d'un administrateur délégué empêche également automatiquement tous les tableaux de bord au niveau de l'organisation créés par cet administrateur délégué d'agréger de nouvelles métriques de stockage.

Pour plus d'informations, consultez Amazon S3 Storage Lens et AWS Organizations dans le Guide de l'utilisateur AWS Organizations .

Rôles liés à un service Amazon S3 Storage Lens

Outre l'accès AWS Organizations sécurisé, Amazon S3 Storage Lens utilise des rôles liés à un service AWS Identity and Access Management (IAM). Un rôle lié à un service est un type unique de rôle IAM lié directement au S3 Storage Lens. Les rôles liés à un service sont prédéfinis par S3 Storage Lens et incluent toutes les autorisations nécessaires pour collecter les métriques de stockage et d'activité quotidiennes des comptes membres de votre organisation.

Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon S3 Storage Lens.

Glossaire des métriques Amazon S3 Storage Lens

Le glossaire des métriques Amazon S3 Storage Lens fournit la liste complète des métriques gratuites et avancées pour S3 Storage Lens.

S3 Storage Lens offre des métriques gratuites pour tous les tableaux de bord et configurations, avec la possibilité d'une mise à niveau vers les métriques avancées.

- Les métriques gratuites contiennent des métriques pertinentes pour l'utilisation de votre stockage, telles que le nombre de compartiments et les objets dans votre compte. Les métriques gratuites incluent également des métriques basées sur des cas d'utilisation, telles que les métriques sur l'optimisation des coûts et la protection des données. Toutes les métriques gratuites sont collectées quotidiennement et les données sont disponibles pour les requêtes jusqu'à 14 jours.
- Les métriques et recommandations avancées incluent toutes les métriques gratuites et des métriques supplémentaires, telles que les métriques avancées sur la protection des données et l'optimisation des coûts. Les métriques avancées incluent également des catégories de métriques supplémentaires, telles que les métriques d'activité et les métriques de codes de statut détaillées. Les métriques avancées sont disponibles pour les requêtes pendant 15 mois.

  Des frais supplémentaires sont facturés lorsque vous utilisez S3 Storage Lens avec des métriques et recommandations avancées. Pour plus d'informations, consultez Tarification Amazon S3. Pour plus d'informations sur les fonctionnalités des métriques et recommandations avancées, consultez Sélection des métriques.

  > **Note**
  >
  > Pour les groupes Storage Lens, seules les métriques de stockage du niveau d'offre gratuite sont disponibles. Les métriques de niveau avancé ne sont pas disponibles au niveau du groupe Storage Lens.

Noms des métriques

La colonne Nom de la métrique du tableau suivant fournit le nom de chaque métrique de S3 Storage Lens dans la console S3. La colonne CloudWatch and export fournit le nom de chaque métrique dans

Amazon CloudWatch et le fichier d'exportation des métriques que vous pouvez configurer dans votre tableau de bord S3 Storage Lens.

Formules de métriques dérivées

Les mesures dérivées ne sont pas disponibles pour l'exportation des mesures et l'option de CloudWatch publication. Cependant, vous pouvez utiliser les formules de métriques affichées dans la colonne Formule de métrique dérivée pour les calculer.

Interprétation des symboles de préfixe Amazon S3 Storage Lens des multiples des unités de métriques (K, M, G, etc.)

Les multiples des unités des métriques S3 Storage Lens sont écrits avec des symboles de préfixe. Ces symboles de préfixe correspondent aux symboles du Système international d'unités (SI) normalisés par le Bureau international des poids et mesures (BIPM). Ces symboles sont également utilisés dans le Code unifié des unités de mesure (UCUM). Pour plus d'informations, consultez Liste des symboles de préfixe SI.

> **Note**
>
> - L'unité de mesure des octets de stockage S3 est le gigaoctet binaire (Go), où 1 Go correspond à 2^{30} octets, 1 To à 2^{40} octets et 1 Po à 2^{50} octets. Cette unité de mesure est également connue sous le nom de gibioctet (GiB), selon la définition de la Commission électrotechnique internationale (CEI).
> - Lorsqu'un objet est en fin de vie selon la configuration de son cycle de vie, Amazon S3 le place dans une file d'attente en vue de sa suppression et le supprime de manière asynchrone. Cependant, un certain retard est possible entre la date d'expiration et la date à laquelle Amazon S3 supprime l'objet. S3 Storage Lens n'inclut pas de métriques pour les objets qui ont expiré mais qui n'ont pas été supprimés. Pour plus d'informations sur les actions d'expiration dans le cycle de vie S3, consultez Objets en cours d'expiration.

Le tableau suivant présente le glossaire des métriques S3 Storage Lens.

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Total storage (Stockage total)	StorageBytes	Stockage total, y compris les chargements partitionnés incomplets, les métadonnées des objets et les marqueurs de suppression	Free	Réca atif	N	-
Object count (Nombre d'objets)	ObjectCount	Nombre total d'objets	Free	Réca atif	N	-
Average object size (Taille moyenne des objets)	-	Taille moyenne des objets	Free	Réca atif	Y	somme (StorageBytes) / somme () ObjectCount
Active buckets (Compartiments actifs)	-	Nombre total de compartiments disposant d'un stockage supérieur à 0 octet	Free	Réca atif	Y	-
Compartiments	-	Nombre total de compartiments	Free	Réca atif	Y	-
Comptes	-	Nombre de comptes dont le	Free	Réca atif	Y	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
		stockage est dans la portée				
Octets de version actuelle	CurrentVersionStorageBytes	Nombre d'octets qui sont une version actuelle d'un objet	Free	Optii ion des coût	N	-
% d'octets de version actuelle	-	Pourcentage d'octets dans la portée qui sont des versions actuelles d'objets	Free	Optii ion des coût	Y	somme (CurrentVersionStorageBytes) / somme () StorageBytes
Nombre d'objets de version actuelle	CurrentVersionObjectCount	Nombre d'objets d'une version actuelle	Free	Prot n des donr	N	-
% current version objects (% d'objets de version actuelle)	-	Pourcentage d'objets dans l'étendue qui correspondent à une version actuelle	Free	Optii ion des coût	Y	somme (CurrentVersionObjectCount) / somme () ObjectCount

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Octets de version ancienne	NonCurrentVersionStorageBytes	Nombre d'octets de version ancienne	Free	Option des coût	N	-
% d'octets de version ancienne	-	Pourcentage d'octets dans la portée qui sont des versions non actuelles	Free	Option des coût	Y	somme (NonCurrentVersionStorageBytes) / somme () StorageBytes
Nombre d'objets de version ancienne	NonCurrentVersionObjectCount	Nombre des versions d'objet anciennes	Free	Option des coût	N	-
% noncurrent version objects (% d'objets de version ancienne)	-	Pourcentage d'objets dans la portée d'une version non actuelle	Free	Option des coût	Y	somme (NonCurrentVersionObjectCount) / somme () ObjectCount

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Octets de marqueur de suppression	DeleteMarkerStorageBytes	Nombre d'octets dans la portée qui sont des marqueurs de suppression	Free	Optii ion des coût	N	-
% d'octets de marqueur de suppression	-	Pourcentage d'octets dans la portée qui sont des marqueurs de suppression	Free	Optii ion des coût	Y	somme (DeleteMarkerStorageBytes) / somme () StorageBytes
Nombre d'objets marqueur de suppression	DeleteMarkerObjectCount	Nombre total d'objets avec un marqueur de suppression	Free	Optii ion des coût	N	-
% delete marker objects (% d'objets marqueur de suppression)	-	Pourcentage d'objets dans la portée avec un marqueur de suppression	Free	Optii ion des coût	Y	somme (DeleteMarkerObjectCount) / somme () ObjectCount

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Octets de chargements partitionnés non terminés	IncompleteMultipartUploadStorageBytes	Nombre total d'octets dans la portée pour des chargements partitionnés non terminés	Free	Option des coût	N	-
% d'octets de chargements partitionnés non terminés	-	Pourcentage d'octets dans la portée qui sont le résultat de chargements partitionnés non terminés	Free	Option des coût	Y	somme (IncompleteMultipartUploadStorageBytes) / somme () StorageBytes
Nombre d'objets de chargement partitionné non terminés	IncompleteMultipartUploadObjectCount	Nombre d'objets dans la portée qui sont des téléchargements partitionnés incomplets	Free	Option des coût	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
% d'objets de chargement partitionné non terminés	-	Pourcentage d'objets dans la portée qui sont des télécharg ements partition nés incomplets	Free	Opti ion des coût	Y	somme (Incomple teMultipa rtUploadO bjectCoun t) / somme () ObjectCou nt
Nombre d'octets de stockage de chargements partitionnés non terminés datant de plus de 7 jours	MPUStorag eBytesOld erThan7 jours incomplets	Nombre total d'octets dans la portée pour des chargements partitionnés non terminés datant de plus de 7 jours	Free	Opti ion des coût	N	-
% d'octets de stockage de chargements partitionnés non terminés datant de plus de 7 jours	-	Pourcentage d'octets pour des chargements partitionnés non terminés datant de plus de 7 jours	Free	Opti ion des coût	Y	sum (MPUStora geBytesOl derThan7 jours incomplet s) / sum () StorageBy tes

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Nombre d'objets de chargement partitionné non terminés datant de plus de 7 jours	MPUObjectCountOlderThan7 jours incomplets	Nombre d'objets qui sont des chargements partitionnés non terminés datant de plus de 7 jours	Free	Option des coût	N	-
% d'objets de chargement partitionné non terminés datant de plus de 7 jours	-	Pourcentage d'objets qui sont des chargements partitionnés non terminés datant de plus de 7 jours	Free	Option des coût	Y	sum (MPUObjectCountOlderThan7 jours incomplets) / sum () ObjectCount
Nombre de règles de cycle de vie de transition	TransitionLifecycleRuleCount	Nombre de règles de cycle de vie permettant de transférer des objets vers une autre classe de stockage	Avan	Option des coût	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Average transition lifecycle rules per bucket (Nombre moyen de règles de cycle de vie de transition par compartiment)	-	Nombre moyen de règles de cycle de vie permettant de transférer des objets vers une autre classe de stockage	Avan	Opti ion des coût	Y	somme (Transiti onLifecyc leRuleCou nt) / somme () DistinctN umberOfBu ckets
Nombre de règles de cycle de vie d'expirat ion	Expiratio nLifecycl eRuleCount	Nombre de règles de cycle de vie servant à faire expirer les objets	Avan	Opti ion des coût	N	-
Average expiration lifecycle rules per bucket (Nombre moyen de règles de cycle de vie d'expiration par compartiment)	-	Nombre moyen de règles de cycle de vie servant à faire expirer les objets	Avan	Opti ion des coût	Y	somme (Expirati onLifecyc leRuleCou nt) / somme () DistinctN umberOfBu ckets

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Nombre de règles de cycle de vie des transitions de version ancienne	NoncurrentVersionTransitionLifecycleRuleCount	Nombre de règles de cycle de vie permettant de transférer des versions d'objet anciennes vers une autre classe de stockage	Avan	Option des coût	N	
Average noncurrent version transition lifecycle rules per bucket (Nombre moyen de règles de cycle de vie de transition de version ancienne par compartiment)	-	Nombre moyen de règles de cycle de vie permettant de transférer des versions d'objet anciennes vers une autre classe de stockage	Avan	Option des coût	Y	somme (NoncurrentVersionTransitionLifecycleRuleCount) / somme () DistinctNumberOfBuckets
Nombre de règles de cycle de vie d'expiration de version ancienne	NoncurrentVersionExpirationLifecycleRuleCount	Nombre de règles de cycle de vie servant à faire expirer des versions d'objet anciennes	Avan	Option des coût	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Average noncurrent version expiration lifecycle rules per bucket (Nombre moyen de règles de cycle de vie d'expiration de version ancienne par compartiment)	-	Nombre moyen de règles de cycle de vie servant à faire expirer des versions d'objet anciennes	Avan	Optii ion des coût	Y	somme (NoncurrentVersionExpirationLifecycleRuleCount) / somme () DistinctNumberOfBuckets
Abort incomplete multipart upload lifecycle rule count (Nombre de règles de cycle de vie d'abandon de chargements partitionnés non terminés)	AbortIncompleteMPULifecycleRuleCount	Nombre de règles de cycle de vie servant à supprimer les chargements partitionnés non terminés	Avan	Optii ion des coût	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Average abort incomplete multipart upload lifecycle rules per bucket (Nombre moyen de règles de cycle de vie d'abandon de chargements partitionnés non terminés par compartiment)	-	Nombre moyen de règles de cycle de vie servant à supprimer les chargements partitionnés non terminés	Avan	Optii ion des coût	Y	somme (AbortIncompleteMPULifecycleRuleCount) / somme () DistinctNumberOfBuckets
Nombre de règles de cycle de vie des marqueurs de suppression d'objets expirés	ExpiredObjectDeleteMarkerLifecycleRuleCount	Nombre de règles de cycle de vie pour supprimer les marqueurs de suppression des objets expirés	Avan	Optii ion des coût	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Average expired object delete marker lifecycle rules per bucket (Nombre moyen de règles de cycle de vie des marqueurs de suppression d'objets expirés par compartiment)	-	Nombre moyen de règles de cycle de vie servant à supprimer les marqueurs de suppression des objets expirés	Avan	Optin des coût	Y	somme (ExpiredObjectDeleteMarkerLifecycleRuleCount) / somme () DistinctNumberOfBuckets
Nombre total de règles de cycle de vie	TotalLifecycleRuleCount	Nombre total de règles de cycle de vie	Avan	Optin des coût	N	-
Average lifecycle rule count per bucket (Nombre moyen de règles de cycle de vie par compartiment)	-	Nombre moyen de règles de cycle de vie	Avan	Optin des coût	Y	somme (TotalLifecycleRuleCount) / somme () DistinctNumberOfBuckets

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Octets chiffrés	Encrypted StorageBytes	Nombre total d'octets chiffrés	Free	Prot n des donr	N	-
% d'octets chiffrés	-	Pourcentage du total des octets chiffrés	Free	Prot n des donr	Y	somme (EncryptedObjectCount) / somme () StorageBytes
Nombre d'objets chiffrés	Encrypted ObjectCount	Nombre total d'objets chiffrés	Free	Prot n des donr	N	-
% encrypted objects (% d'objets chiffrés)	-	Pourcentage des objets chiffrés	Free	Prot n des donr	Y	somme (EncryptedStorageBytes) / somme () ObjectCount

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté [2]	D	Form de métr dériv
Octets non chiffrés	UnencryptedStorageBytes	Nombre d'octets qui ne sont pas chiffrés	Free	Prot n des donr	Y	somme (StorageBytes) - somme (EncryptedStorageBytes)
% d'octets non chiffrés	-	Pourcentage d'octets qui ne sont pas chiffrés	Free	Prot n des donr	Y	somme (UnencryptedStorageBytes) / somme () StorageBytes
Nombre d'objets non chiffrés	UnencryptedObjectCount	Nombre total d'objets non chiffrés	Free	Prot n des donr	Y	somme (ObjectCount) - somme (EncryptedObjectCount)

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
% d'objets non chiffrés	-	Pourcentage d'objets non chiffrés	Free	Prot n des donr	Y	somme (Unencrypt edStorag eBytes) / somme () ObjectCou nt
Source d'octets de stockage répliqués	Replicate dStorageB ytesSource	Nombre total d'octets répliqués à partir du compartiment source	Free	Prot n des donr	N	-
% replicated bytes source (Source en % d'octets répliqués)	-	Pourcentage du nombre total d'octets répliqués à partir du compartiment source	Free	Prot n des donr	Y	somme (Replicat edStorage BytesSour ce) / somme () StorageBy tes
Source du nombre d'objets répliqués	Replicate dObjectCo untSource	Nombre d'objets répliqués à partir du compartiment source	Free	Prot n des donr	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
% replicated objects source (Source en % d'objets répliqués)	-	Pourcentage du nombre total d'objets répliqués à partir du compartiment source	Free	Prot n des donr	Y	somme (ReplicatedStorageObjectCount) / somme () ObjectCount
Destination des octets de stockage répliqués	ReplicatedStorageBytes	Nombre total d'octets répliqués vers le compartiment de destination	Free	Prot n des donr	N	-
% replicated bytes destination (Destination en % d'octets répliqués)	-	Pourcentage du nombre total d'octets répliqués vers le compartiment de destination	Free	Prot n des donr	Y	somme (ReplicatedStorageBytes) / somme () StorageBytes
Replicated object count destination (Destination du nombre d'objets répliqués)	ReplicatedObjectCount	Nombre d'objets répliqués vers le compartiment de destination	Free	Prot n des donr	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
% replicated objects destination (Destination en % des objets répliqués)	-	Pourcentage du nombre total d'objets répliqués vers le compartiment de destination	Free	Prot n des donr	Y	somme (ReplicatedObjectCount) / somme () ObjectCount
Octets de verrouillage d'objets	ObjectLockEnabledStorageBytes	Nombre total d'octets de stockage avec verrouillage d'objets activé	Free	Prot n des donr	N	somme (UnencryptedStorageBytes) / somme (ObjectLockEnabledStorageCount) - somme () ObjectLockEnabledStorageBytes

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
% d'octets de verrouillage d'objets	-	Pourcentage d'octets de stockage avec verrouillage d'objets activé	Free	Prot n des donr	Y	somme (ObjectLo ckEnabled StorageBy tes) / somme () StorageBy tes
Nombre d'objets de verrouillage d'objet	ObjectLoc kEnabledO bjectCount	Nombre total d'objets de verrouillage d'objets	Free	Prot n des donr	N	-
% d'objets de verrouillage d'objet	-	Pourcentage du nombre total d'objets pour lesquels le verrouillage d'objets est activé	Free	Prot n des donr	Y	somme (ObjectLo ckEnabled ObjectCou nt) / somme () ObjectCou nt
Versioning-enabled bucket count (Nombre de compartim ents activés pour la gestion des versions)	Versionin gEnabledB ucketCount	Nombre de compartiments pour lesquels la gestion des versions S3 est activée	Free	Prot n des donr	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
% versioning-enabled buckets (% de compartiments activés pour la gestion des versions)	-	Pourcentage de compartiments pour lesquels la gestion des versions S3 est activée	Free	Prot n des donr	Y	somme (VersioningEnabledBucketCount) / somme () DistinctNumberOfBuckets
MFA delete-enabled bucket count (Nombre de compartiments activés pour la suppression MFA)	MFADeleteEnabledBucketCount	Nombre de compartiments pour lesquels la suppression MFA (authentification multifactorielle) est activée	Free	Prot n des donr	N	-
% MFA delete-enabled buckets (% de compartiments avec suppression MFA activée)	-	Pourcentage de compartiments pour lesquels la suppression MFA (authentification multifactorielle) est activée	Free	Prot n des donr	Y	somme (MFADeleteEnabledBucketCount) / somme () DistinctNumberOfBuckets

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
SSE-KMS enabled bucket count (Nombre de compartiments avec SSE-KMS activé)	SSEKMSEnabledBucketCount	Nombre de compartiments qui utilisent le chiffrement côté serveur à l'aide de AWS Key Management Service clés (SSE-KMS) pour le chiffrement des compartiments par défaut	Free	Proto n des donr	N	-
% SSE-KMS enabled buckets (% de compartiments avec SSE-KMS activé)	-	Pourcentage de compartiments utilisant le protocole SSE-KMS pour le chiffrement des compartiments par défaut	Free	Proto n des donr	Y	somme (SSEKMSEnabledBucketCount) / somme () DistinctNumberOfBuckets
Toutes les demandes de signature non prises en charge	AllUnsupportedSignatureRequests	Le nombre total de demandes utilisant des versions de AWS signature non prises en charge	Avan	Proto n des donr	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
% de toutes les demandes de signature non prises en charge	-	Pourcentage de demandes utilisant des versions de AWS signature non prises en charge	Avan	Prot n des donr	Y	somme (AllUnsupportedSignatureRequests) / somme () AllRequests
Toutes les demandes TLS non prises en charge	AllUnsupportedTLSRequests	Nombre de demandes qui utilisent des versions de protocole TLS (Transport Layer Security) non prises en charge	Avan	Prot n des donr	N	-
% de toutes les demandes TLS non prises en charge	-	Pourcentage de demandes qui utilisent des versions TLS non prises en charge	Avan	Prot n des donr	Y	somme (AllUnsupportedTLSRequests) / somme () AllRequests

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Toutes les demandes SSE-KMS	Tout SSEKMSReq uests	Nombre total de demandes spécifiant le protocole SSE-KMS	Avan	Prot n des donr	N	-
% de toutes les demandes SSE-KMS	-	Pourcentage de demandes qui spécifient le protocole SSE-KMS	Avan	Prot n des donr	Y	somme (ToutSSEK MSRequest s) / somme () AllReques ts
Nombre de règles de réplication pour la même région	SameRegio nReplicat ionRuleCount	Nombre de règles de la réplication pour la réplication dans une même région (SRR)	Avan	Prot n des donr	N	-
Nombre moyen de règles de réplication pour la même région par compartim ent	-	Nombre moyen de règles de réplication pour la réplication dans une même région (SRR)	Avan	Prot n des donr	Y	somme (SameRegi onReplica tionRuleC ount) / somme () DistinctN umberOfBu ckets

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Nombre de règles de réplication entre régions	CrossRegionReplicationRuleCount	Nombre de règles de réplication pour la réplication entre régions (CRR)	Avan	Prot n des donr	N	-
Nombre moyen de règles de réplication entre régions par compartiment	-	Nombre moyen de règles de réplication pour la réplication entre régions (CRR)	Avan	Prot n des donr	Y	somme (CrossRegionReplicationRuleCount) / somme () DistinctNumberOfBuckets
Same-account replication rule count (Nombre de règles de réplication pour le même compte)	SameAccountReplicationRuleCount	Nombre de règles de réplication pour la réplication au sein du même compte	Avan	Prot n des donr	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Average same-account replication rules per bucket (Nombre moyen de règles de réplication pour le même compte par compartiment)	-	Nombre moyen de règles de réplicati on pour la réplicati on au sein du même compte	Avan	Prot n des donr	Y	somme (SameAcco untReplic ationRule Count) / somme () DistinctN umberOfBu ckets
Cross-account replication rule count (Nombre de règles de réplication entre comptes)	CrossAcco untReplic ationRuleCount	Nombre de règles de réplication pour la réplication entre comptes	Avan	Prot n des donr	N	-
Average cross-account replication rules per bucket (Nombre moyen de règles de réplication entre comptes par compartim ent)	-	Nombre moyen de règles de réplicati on pour la réplicati on entre comptes	Avan	Prot n des donr	Y	somme (CrossAcc ountRepli cationRul eCount) / somme () DistinctN umberOfBu ckets

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Nombre de règles de réplication de destination non valide	InvalidDestination ReplicationRuleCount	Nombre de règles de réplication dont la destination de réplication n'est pas valide	Avan	Prot n des donr	N	-
Average invalid destination replication rules per bucket (Nombre moyen de règles de réplication de destination non valide par compartiment)	-	Nombre moyen de règles de réplication dont la destination de réplication n'est pas valide	Avan	Prot n des donr	Y	somme (InvalidReplicationRuleCount) / somme () DistinctNumberOfBuckets
Total replication rule count (Nombre total de règles de réplication)	-	Nombre total de règles de réplication	Avan	Prot n des donr	Y	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Average replication rule count per bucket (Nombre moyen de règles de réplication par compartiment)	-	Nombre total moyen de règles de réplication	Avan	Prot n des donr	Y	sum (toutes les métriques relatives au nombre de règles de réplicati on) / sum (Distinct NumberOfB uckets)
Nombre de compartiments avec propriété d'objets Appliqué par le propriétaire du compartiment	ObjectOwn ershipBuc ketOwnerE nforcedBu cketCount	Nombre total de compartim ents dont les listes de contrôle d'accès (ACLs) sont désactivé es en utilisant le paramètre imposé par le propriétaire du compartiment pour la propriété des objets	Free	Gest des accè	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
% Object Ownership bucket owner enforced buckets (% de compartiments avec propriété d'objets Appliqué par le propriétaire du compartiment)	-	Le pourcentage de buckets qui ont été ACLs désactivés en utilisant le paramètre imposé par le propriétaire du bucket pour la propriété des objets	Free	Gest des accè	Y	somme (ObjectOwnershipBucketOwnerEnforcedBucketCount) / somme () DistinctNumberOfBuckets
Nombre de compartiments avec propriété d'objets Préféré par le propriétaire du compartiment	ObjectOwnershipBucketOwnerPreferredBucketCount	Nombre total de compartiments qui utilisent le paramètre Préféré par le propriétaire du compartiment pour la propriété d'objets	Free	Gest des accè	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
% Object Ownership bucket owner preferred buckets (% de compartiments avec propriété d'objets Préféré par le propriétaire du compartiment)	-	Pourcentage de compartiments qui utilisent le paramètre Préféré par le propriétaire du compartiment pour la propriété d'objets	Free	Gest des accè	Y	somme (ObjectOwnershipBucketOwnerPreferredBucketCount) / somme () DistinctNumberOfBuckets
Nombre de compartiments de l'enregistreur d'objets de la propriété d'objets	ObjectOwnershipObjectWriterBucketCount	Nombre total de compartiments qui utilisent le paramètre d'enregistreur d'objets pour la propriété d'objets	Free	Gest des accè	N	-
% Object Ownership object writer buckets (% de compartiments de l'enregistreur d'objets de la propriété d'objets)	-	Pourcentage de compartiments qui utilisent le paramètre d'enregistreur d'objets pour la propriété d'objets	Free	Gest des accè	Y	somme (ObjectOwnershipObjectWriterBucketCount) / somme () DistinctNumberOfBuckets

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
Nombre de compartiments activés pour l'accélération de transfert	TransferAccelerationEnabledBucketCount	Nombre total de compartiments pour lesquels l'accélération de transfert est activée	Free	Perf ces	N	-
% Transfer Acceleration enabled buckets (Pourcentage de compartiments activés pour l'accélération de transfert)	-	Pourcentage de compartiments pour lesquels l'accélération de transfert est activée	Free	Perf ces	Y	somme (TransferAccelerationEnabledBucketCount) / somme () DistinctNumberOfBuckets
Nombre de compartiments activés par notification d'événements	EventNotificationEnabledBucketCount	Nombre total de compartiments pour lesquels les notifications d'événements sont activées	Free	Évér s	N	

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
% Event Notification enabled buckets (% de compartiments activés par notification d'événements)	-	Pourcentage de compartiments pour lesquels les notifications d'événements sont activées	Free	Évér s	Y	somme (EventNotification EnabledBucketCount) / somme () DistinctNumberOfBuckets
Toutes les demandes	AllRequests	Nombre total de requêtes effectuées	Avan	Activ	N	-
Demandes Get	GetRequests	Nombre total de requêtes `GET` effectuées	Avan	Activ	N	-
Demandes PUT	PutRequests	Nombre total de requêtes `PUT` effectuées	Avan	Activ	N	-
Demandes HEAD	HeadRequests	Nombre total de requêtes `HEAD` effectuées	Avan	Activ	N	-
Demandes DELETE	DeleteRequests	Nombre total de requêtes `DELETE` effectuées	Avan	Activ	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Demandes List	ListRequests	Nombre total de requêtes `LIST` effectuées	Avan	Activ	N	-
Demandes POST	PostRequests	Nombre total de requêtes `POST` effectuées	Avan	Activ	N	-
Demandes SELECT	SelectRequests	Nombre total de demandes S3 SELECT	Avan	Activ	N	-
Octets de sélection analysés	SelectScannedBytes	Nombre d'octets de sélection S3 analysés	Avan	Activ	N	-
Octets de sélection retournés	SelectReturnedBytes	Nombre d'octets de sélection S3 retournés	Avan	Activ	N	-
Octets téléchargés	BytesDownloaded	Nombre d'octets téléchargés	Avan	Activ	N	-
% retrieval rate (Taux d'extraction en %)	-	Pourcentage d'octets téléchargés	Avan	Activ	Y	somme (BytesDownloaded) / somme () StorageBytes
Octets chargés	BytesUploaded	Nombre d'octets chargés	Avan	Activ	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métr dériv
% ingest ratio (Ratio d'ingestion en %)	-	Pourcentage d'octets chargés	Avan	Activ	Y	somme (BytesUploaded) / somme () StorageBytes
Erreurs 4xx	4xxErrors	Nombre total de codes de statut HTTP 4xx	Avan	Activ	N	-
Erreurs 5xx	5xxErrors	Nombre total de codes de statut HTTP 5xx	Avan	Activ	N	-
Total errors (Nombre total d'erreurs)	-	Somme de toutes les erreurs 4xx et 5xx	Avan	Activ	Y	sum(4xxErrors) + sum(5xxErrors)
% error rate (Taux d'erreurs en %)	-	Nombre total d'erreurs 4xx et 5xx exprimé en pourcentage du nombre total de demandes	Avan	Activ	Y	somme (TotalErrors) / somme () TotalRequests

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Nombre de codes de statut 200 OK	200 OKStatus unités	Nombre total de codes de statut 200 OK	Avan	Cod de statu déta	N	-
% 200 OK status (% de codes de statut 200 OK)	-	Nombre total de codes de statut 200 OK sous la forme d'un pourcentage du nombre total de demandes	Avan	Cod de statu déta	Y	somme (200 OKStatus points) / somme () AllReques ts
Nombre de codes de statut 206 Contenu partiel	206 PartialCo ntentStat usCount	Nombre total de codes de statut 206 Contenu partiel	Avan	Cod de statu déta	N	-
% 206 Partial Content status (% de codes de statut 206 Contenu partiel)	-	Nombre total de codes de statut 206 Contenu partiel sous la forme d'un pourcentage du nombre total de demandes	Avan	Cod de statu déta	Y	somme (206Parti alContent StatusCou nt) / somme () AllReques ts

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
Nombre d'erreurs 400 Requête erronée	400 BadReques tErrorCount	Nombre total de codes de statut 400 Requête erronée	Avan	Cod de statu déta	N	-
% 400 Bad Request errors (% d'erreurs 400 Requête erronée)	-	Nombre total de codes de statut 400 Requête erronée sous la forme d'un pourcentage du nombre total de demandes	Avan	Cod de statu déta	Y	somme (400BadRe questErro rCount) / somme () AllReques ts
Nombre d'erreurs 403 Forbidden	403 Forbidden ErrorCount	Nombre total de codes de statut 403 Forbidden	Avan	Cod de statu déta	N	-
% d'erreurs 403 Forbidden	-	Nombre total de codes de statut 403 Forbidden sous la forme d'un pourcentage du nombre total de demandes	Avan	Cod de statu déta	Y	somme (403Forbi ddenError Count) / somme () AllReques ts
Nombre d'erreurs 404 Non trouvé	404 NotFoundE rrorCount	Nombre total de codes de statut 404 Non trouvé	Avan	Cod de statu déta	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté[2]	D	Form de métri dériv
% 404 Not Found errors (% d'erreurs 404 Non trouvé)	-	Nombre total de codes de statut 404 Non trouvé sous la forme d'un pourcentage du nombre total de demandes	Avan	Cod de statu déta	Y	somme (404NotFoundErrorCount) / somme () AllRequests
Nombre de codes 500 Erreur de serveur interne	500 InternalServerErrorCount	Nombre total de codes de statut 500 Erreur de serveur interne	Avan	Cod de statu déta	N	-
% 500 Internal Server Errors (% d'erreurs 500 Erreur de serveur interne)	-	Nombre total de codes de statut 500 Erreur de serveur interne sous la forme d'un pourcentage du nombre total de demandes	Avan	Cod de statu déta	Y	somme (500InternalServerErrorCount) / somme () AllRequests
Nombre d'erreurs 503 Service non disponible	503 ServiceUnavailableErrorCount	Nombre total de codes de statut 503 Service non disponible	Avan	Cod de statu déta	N	-

Nom de la métrique	CloudWatch et exportation	Description	Nive	Caté [2]	D	Form de métri dériv
% 503 Service Unavailable errors (% d'erreurs 503 Service non disponible)	-	Nombre total de codes de statut 503 Service non disponible sous la forme d'un pourcentage du nombre total de demandes	Avan	Cod de statu déta	Y	somme (503ServiceUnavailableError Count) / somme () AllRequests

[1] Toutes les métriques de stockage du niveau d'offre gratuite sont disponibles au niveau du groupe Storage Lens. Les métriques de niveau avancé ne sont pas disponibles au niveau du groupe Storage Lens.

[2] Les métriques relatives au nombre de règles et aux paramètres des compartiments ne sont pas disponibles au niveau du préfixe.

Définition d'autorisations Amazon S3 Storage Lens

Amazon S3 Storage Lens nécessite de nouvelles autorisations dans AWS Identity and Access Management (IAM) pour autoriser l'accès aux actions S3 Storage Lens. Pour accorder ces autorisations, vous pouvez utiliser une politique IAM basée sur l'identité. Vous pouvez attacher cette politique aux utilisateurs, groupes ou rôles IAM pour leur accorder des autorisations. Ces autorisations peuvent inclure la possibilité d'activer ou de désactiver S3 Storage Lens ou d'accéder à n'importe quel tableau de bord ou n'importe quelle configuration S3 Storage Lens.

L'utilisateur ou le rôle IAM doit appartenir au compte qui a créé ou qui détient le tableau de bord ou la configuration, sauf si les deux conditions suivantes sont remplies :

- Votre compte est membre de AWS Organizations.
- Vous avez été autorisé à créer des tableaux de bord au niveau de l'organisation par votre compte de gestion en tant qu'administrateur délégué.

> **Note**
>
> - Vous ne pouvez pas utiliser les informations d'identification de l'utilisateur root de votre compte pour afficher les tableaux de bord Amazon S3 Storage Lens. Pour accéder aux tableaux de bord S3 Storage Lens, vous devez accorder les autorisations IAM requises à un utilisateur IAM nouveau ou existant. Connectez-vous ensuite à l'aide de ces informations d'identification utilisateur pour accéder aux tableaux de bord S3 Storage Lens. Pour plus d'informations, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.
> - L'utilisation de S3 Storage Lens sur la console Amazon S3 peut nécessiter plusieurs autorisations. Par exemple, pour modifier un tableau de bord sur la console, vous devez disposer des autorisations suivantes :
>   - `s3:ListStorageLensConfigurations`
>   - `s3:GetStorageLensConfiguration`
>   - `s3:PutStorageLensConfiguration`

Rubriques

- Définir des autorisations de compte pour utiliser S3 Storage Lens
- Définition d'autorisations de compte pour utiliser des groupes S3 Storage Lens
- Configuration des autorisations pour utiliser S3 Storage Lens avec AWS Organizations

Définir des autorisations de compte pour utiliser S3 Storage Lens

Pour créer et gérer des tableaux de bord S3 Storage Lens et des configurations de tableau de bord Storage Lens, vous devez disposer des autorisations suivantes, en fonction des opérations que vous souhaitez effectuer :

Le tableau suivant présente les autorisations IAM liées à Amazon S3 Storage Lens.

Action	Autorisations IAM
Créez ou mettez à jour un tableau de bord S3 Storage Lens dans la console Amazon S3.	`s3:ListStorageLensConfigurations` `s3:GetStorageLensConfiguration`

Action	Autorisations IAM

	`s3:GetStorageLensConfigurationTagging`
	`s3:PutStorageLensConfiguration`
	`s3:PutStorageLensConfigurationTagging`

Obtenez les étiquettes d'un tableau de bord S3 Storage Lens sur la console Amazon S3.	`s3:ListStorageLensConfigurations` `s3:GetStorageLensConfigurationTagging`

Affichez un tableau de bord S3 Storage Lens sur la console Amazon S3.	`s3:ListStorageLensConfigurations`
	`s3:GetStorageLensConfiguration`
	`s3:GetStorageLensDashboard`

Supprimez un tableau de bord S3 Storage Lens sur la console Amazon S3.	`s3:ListStorageLensConfigurations`
	`s3:GetStorageLensConfiguration`
	`s3:DeleteStorageLensConfiguration`

Créez ou mettez à jour une configuration S3 Storage Lens à l'aide du AWS CLI ou d'un AWS SDK.	`s3:PutStorageLensConfiguration` `s3:PutStorageLensConfigurationTagging`
Obtenez les balises d'une configuration S3 Storage Lens à l'aide du AWS CLI ou d'un AWS SDK.	`s3:GetStorageLensConfigurationTagging`
Affichez une configuration S3 Storage Lens à l'aide du AWS CLI ou d'un AWS SDK.	`s3:GetStorageLensConfiguration`

Action	Autorisations IAM
Supprimez une configuration S3 Storage Lens à l'aide du AWS SDK AWS CLI ou.	`s3:DeleteStorageLensConfiguration`

> **Note**
>
> - Vous pouvez utiliser des balises de ressources dans une politique IAM pour gérer les autorisations.
> - Un rôle ou un utilisateur IAM disposant de ces autorisations peut voir des métriques à partir de compartiments et de préfixes pour lesquels il peut ne pas avoir d'autorisation directe pour lire ou répertorier les objets.
> - Pour les tableaux de bord S3 Storage Lens sur lesquels les métriques au niveau du préfixe sont activées, si le chemin d'un préfixe sélectionné correspond à une clé d'objet, le tableau de bord peut afficher la clé d'objet sous la forme d'un autre préfixe.
> - Pour les exportations de métriques, qui sont stockées dans un compartiment de votre compte, les autorisations sont accordées à l'aide de l'autorisation `s3:GetObject` existante dans la politique IAM. De même, pour une AWS Organizations entité, le compte de gestion de l'organisation ou les comptes d'administrateur délégué peuvent utiliser les politiques IAM pour gérer les autorisations d'accès pour le tableau de bord et les configurations au niveau de l'organisation.

Définition d'autorisations de compte pour utiliser des groupes S3 Storage Lens

Vous pouvez utiliser les groupes S3 Storage Lens pour comprendre la distribution de votre espace de stockage au sein des compartiments en fonction du préfixe, du suffixe, de la balise d'objet, de la taille de l'objet ou de l'âge de l'objet. Vous pouvez attacher des groupes Storage Lens à vos tableaux de bord pour consulter leurs métriques agrégées.

Pour utiliser des groupes Storage Lens, vous devez disposer de certaines autorisations. Pour de plus amples informations, veuillez consulter the section called "Autorisations pour les groupes Storage Lens".

Configuration des autorisations pour utiliser S3 Storage Lens avec AWS Organizations

Vous pouvez utiliser Amazon S3 Storage Lens pour collecter des métriques de stockage et des données d'utilisation pour tous les comptes qui font partie de votre AWS Organizations hiérarchie. Le tableau suivant présente les actions et les autorisations liées à l'utilisation de S3 Storage Lens avec Organizations.

Action	Autorisations IAM
Activez l'accès sécurisé de S3 Storage Lens à votre organisation.	`organizations:EnableAWSServiceAccess`
Désactivez l'accès approuvé pour S3 Storage Lens pour votre organisation.	`organizations:DisableAWSServiceAccess`
Enregistrez un administrateur délégué pour créer des tableaux de bord ou des configurations S3 Storage Lens pour votre organisation.	`organizations:RegisterDelegatedAdministrator`
Désinscrivez un administrateur délégué afin qu'il ne puisse plus créer de tableaux de bord ni de configurations S3 Storage Lens pour votre organisation.	`organizations:DeregisterDelegatedAdministrator`

Autorisations supplémentaires pour créer des configurations S3 Storage Lens à l'échelle de l'organisation.	`organizations:DescribeOrganization`
	`organizations:ListAccounts`
	`organizations:ListAWSServiceAccessForOrganization`
	`organizations:ListDelegatedAdministrators`
	`iam:CreateServiceLinkedRole`

Utilisation d'Amazon S3 Storage Lens à l'aide de la console et de l'API

Amazon S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Vous pouvez utiliser les métriques S3 Storage Lens pour générer des informations récapitulatives, telles que la quantité de stockage dont vous disposez dans l'ensemble de votre organisation ou les compartiments et préfixes qui connaissent la croissance la plus rapide. Vous pouvez également utiliser les métriques S3 Storage Lens pour identifier les opportunités d'optimisation des coûts, mettre en œuvre les bonnes pratiques de protection et de sécurisation des données et améliorer les performances des charges de travail d'application. Par exemple, vous pouvez identifier les compartiments qui sont dépourvus de règles de cycle de vie S3 pour faire expirer les chargements partitionnés non terminés datant de plus de 7 jours. Vous pouvez également identifier les compartiments qui ne respectent pas les bonnes pratiques de protection des données, telles que l'utilisation de la réplication S3 ou de la gestion des versions S3. S3 Storage Lens analyse également les métriques de stockage pour fournir des recommandations contextuelles afin d'aider à réduire les coûts de stockage et à appliquer les bonnes pratiques de protection des données.

S3 Storage Lens regroupe vos métriques et affiche les informations dans la section Account snapshot (Instantané du compte) sur la page Buckets (Compartiments) de la console Amazon S3. S3 Storage Lens fournit également un tableau de bord interactif que vous pouvez utiliser pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord dispose d'options d'exploration pour générer et visualiser des informations au niveau de l'organisation, du compte, de la Région AWS, de la classe de stockage, du compartiment, du préfixe ou du groupe Storage Lens. Vous pouvez également envoyer une exportation de métriques quotidienne au format CSV ou Parquet vers un compartiment S3.

La section suivante contient des exemples de création, de mise à jour et d'affichage des configurations S3 Storage Lens et d'exécution d'opérations liées à la fonction. Si vous utilisez S3 Storage Lens avec AWS Organizations, ces exemples couvrent également ces cas d'utilisation. Dans les exemples, remplacez les valeurs de variable par celles qui vous conviennent.

Rubriques

- Création d'un tableau de bord Amazon S3 Storage Lens
- Mise à jour d'un tableau de bord Amazon S3 Storage Lens
- Désactivation d'un tableau de bord Amazon S3 Storage Lens
- Suppression d'un tableau de bord Amazon S3 Storage Lens

- Affichage des tableaux de bord Amazon S3 Storage Lens
- Affichage des détails d'un tableau de bord Amazon S3 Storage Lens
- Gestion des balises de AWS ressources avec S3 Storage Lens
- Fichiers d'aide pour l'utilisation d'Amazon S3 Storage Lens

Création d'un tableau de bord Amazon S3 Storage Lens

Vous pouvez créer des tableaux de bord personnalisés S3 Storage Lens supplémentaires qui peuvent être adaptés à votre organisation AWS Organizations ou à des compartiments spécifiques Régions AWS au sein d'un compte.

> **Note**
>
> L'affichage ou la visualisation des mises à jour apportées à la configuration de votre tableau de bord peut prendre jusqu'à 48 heures.

Utilisation de la console S3

Procédure pour créer un tableau de bord Amazon S3 Storage Lens sur la console Amazon S3.

Étape 1 : définir la portée du tableau de bord

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, sélectionnez le nom de la région AWS actuellement affichée. Choisissez ensuite la région à laquelle vous souhaitez passer.
3. Dans le volet de navigation de gauche, sous S3 Storage Lens, choisissez Tableaux de bord.
4. Choisissez Create dashboard (Créer un tableau de bord).
5. Sur la page Tableau de bord, dans la section General (Général), procédez comme suit :

    a. Sélectionnez la région d'origine de votre tableau de bord. La région d'origine est l' Région AWS endroit où sont stockées la configuration et les mesures de ce tableau de bord Storage Lens.

    b. Saisissez un nom de tableau de bord.

Les noms de tableau de bord doivent contenir moins de 65 caractères et ne doivent pas contenir de caractères spéciaux ou d'espaces.

> **Note**
>
> Vous ne pouvez pas modifier ce nom de tableau de bord une fois le tableau de bord créé.

c. Vous pouvez éventuellement choisir d'ajouter des balises à votre tableau de bord. Vous pouvez utiliser des balises pour gérer les autorisations de votre tableau de bord et suivre les coûts relatifs à S3 Storage Lens.

Pour plus d'informations, consultez Contrôle de l'accès à l'aide d'étiquettes de ressources dans le Guide de l'utilisateur IAM et Étiquettes de répartition des coûts générées par AWS dans le Guide de l'utilisateur AWS Billing .

> **Note**
>
> Vous pouvez ajouter jusqu'à 50 balises à votre configuration de tableau de bord.

6. Dans la section Dashboard scope (Portée du tableau de bord), procédez comme suit :

a. Sélectionnez les Régions et les compartiments que vous souhaitez que S3 Storage Lens inclue ou exclue du tableau de bord.

b. Sélectionnez les compartiments dans les Régions sélectionnées que vous souhaitez que S3 Storage Lens inclue ou exclue. Vous pouvez inclure ou exclure des compartiments, mais pas les deux. Cette option n'est pas disponible lorsque vous créez des tableaux de bord au niveau de l'organisation.

> **Note**
>
> - Vous pouvez inclure ou exclure des Régions et des compartiments. Cette option est limitée aux Régions uniquement lors de la création de tableaux de bord au niveau de l'organisation sur les comptes membres de votre organisation.
> - Vous pouvez choisir jusqu'à 50 compartiments à inclure ou exclure.

Étape 2 : configurer la sélection des métriques

1. Dans la section Metrics selection (Sélection de métriques), sélectionnez le type de métriques que vous souhaitez agréger pour ce tableau de bord.

   - Pour inclure des métriques gratuites agrégées au niveau du compartiment et disponibles pour les requêtes pendant 14 jours, choisissez Free Metrics (Métriques gratuites).
   - Pour activer les métriques avancées et d'autres options avancées, choisissez Advanced metrics and recommendations (Métriques et recommandations avancées). Ces options incluent l'agrégation avancée des préfixes, la CloudWatch publication sur Amazon et les recommandations contextuelles. Les données sont disponibles pour les requêtes pendant 15 mois. Les métriques et recommandations avancées entraînent un coût supplémentaire. Pour plus d'informations, consultez Tarification Amazon S3.

     Pour plus d'informations sur les métriques gratuites et avancées, consultez Sélection des métriques.

2. Sous Advanced metrics and recommendations features (Fonctionnalités de métriques et recommandations avancées), sélectionnez les options que vous voulez activer :

   - Advanced metrics (Métriques avancées)
   - CloudWatch publiant
   - Prefix aggregation (Agrégation de préfixes)

   > **Important**
   >
   > Si vous activez l'agrégation de préfixes pour votre configuration S3 Storage Lens, les métriques au niveau du préfixe ne seront pas publiées sur. CloudWatch Seules les métriques S3 Storage Lens au niveau du bucket, du compte et de l'organisation sont publiées sur. CloudWatch

3. Si vous avez activé Advanced metrics (Métriques avancées), sélectionnez les Advanced metrics categories (Catégories de métriques avancées) que vous souhaitez afficher dans votre tableau de bord S3 Storage Lens :

   - Métriques d'activité
   - Detailed status code metrics (Métriques détaillées sur le code de statut)
   - Advanced cost optimization metrics (Métriques avancées sur l'optimisation des coûts)

- Advanced data protection metrics (Métriques avancées sur la protection des données)

Pour plus d'informations sur les catégories de métriques, consultez Catégories de métriques. Pour obtenir une liste complète des métriques, consultez Glossaire des métriques Amazon S3 Storage Lens.

4. Si vous avez choisi d'activer l'agrégation des préfixes, configurez les éléments suivants :

   a. Choisissez la taille minimale du seuil de préfixe pour ce tableau de bord.

      Par exemple, un seuil de préfixe de 5 % indique que les préfixes représentant 5 % ou plus de la taille totale de stockage du compartiment seront agrégés.

   b. Sélectionnez la profondeur de préfixe.

      Ce paramètre indique le nombre maximal de niveaux jusqu'auquel les préfixes sont évalués. La profondeur de préfixe doit être inférieure à 10.

   c. Saisissez un caractère de délimiteur de préfixe.

      Cette valeur est utilisée pour identifier chaque niveau de préfixe. La valeur par défaut dans Amazon S3 est le caractère `/`, mais votre structure de stockage peut utiliser d'autres délimiteurs.

(Facultatif) Étape 3 : exporter des métriques pour le tableau de bord

1. Dans la section Metrics export (Exportation de métriques), choisissez Enable (Activer) pour créer une exportation de métriques qui sera placée quotidiennement dans un compartiment de destination de votre choix.

   L'exportation des métriques est au format CSV ou Apache Parquet. La portée des données est la même que celle des données de votre tableau de bord S3 Storage Lens sans les recommandations.

2. Si vous avez activé l'exportation de métriques, choisissez le format de sortie de votre exportation quotidienne de métriques : CSV ou Apache Parquet.

   Parquet est un format de fichier open source pour Hadoop, qui stocke les données imbriquées dans un format en colonnes plat.

3. Sélectionnez le compartiment S3 de destination pour l'exportation de vos métriques.

Vous pouvez choisir un compartiment dans le compte actuel du tableau de bord S3 Storage Lens. Vous pouvez également en choisir un autre Compte AWS si vous disposez des autorisations du compartiment de destination et de l'ID de compte du propriétaire du compartiment de destination.

4. Choisissez le compartiment S3 de destination (format : `s3://bucket-name/prefix`).

   Le compartiment doit être dans la région d'origine de votre tableau de bord S3 Storage Lens. La console S3 vous montre le paramètre Destination bucket permission (Autorisation de compartiment de destination) qui sera ajouté par Amazon S3 à la politique de compartiment de destination. Amazon S3 met à jour la politique de compartiment sur le compartiment de destination pour permettre à S3 de placer des données dans ce compartiment.

5. (Facultatif) Pour activer le chiffrement côté serveur pour l'exportation de vos métriques, choisissez Specify an encryption key (Spécifier une clé de chiffrement). Ensuite, choisissez le Type de chiffrement : Clés gérées par Amazon S3 (SSE-S3) ou Clé AWS Key Management Service (SSE-KMS).

   Vous pouvez choisir entre une clé gérée par Amazon S3 (SSE-S3) et une clé AWS Key Management Service (AWS KMS) (SSE-KMS).

6. (Facultatif) Pour spécifier une AWS KMS clé, vous devez choisir une clé KMS ou saisir une clé Amazon Resource Name (ARN).

   Si vous choisissez une clé gérée par le client, vous devez accorder à S3 Storage Lens l'autorisation de chiffrer dans la politique de clé AWS KMS . Pour de plus amples informations, veuillez consulter Utilisation d'un AWS KMS key pour chiffrer vos exportations de métriques.

7. Choisissez Create dashboard (Créer un tableau de bord).

À l'aide du AWS CLI

Example

L'exemple de commande suivant crée une configuration Amazon S3 Storage Lens avec des balises. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

Example

L'exemple de commande suivant crée une configuration Amazon S3 Storage Lens sans balises. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

```
aws s3control put-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json
```

Utilisation du AWS SDK pour Java

Example – Créer et mettre à jour une configuration Amazon S3 Storage Lens

L'exemple suivant crée et met à jour une configuration Amazon S3 Storage Lens dans le kit SDK pour Java :

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
```

```
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        String exportAccountId = "Destination Account ID";
        String exportBucketArn = "arn:aws:s3:::destBucketName"; // The destination
 bucket for your metrics export must be in the same Region as your S3 Storage Lens
 configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
```

```
                .withBucketLevel(bucketLevel);

        Include include = new Include()
                .withBuckets(Arrays.asList("arn:aws:s3:::bucketName"))
                .withRegions(Arrays.asList("us-west-2"));

        StorageLensDataExportEncryption exportEncryption = new
StorageLensDataExportEncryption()
                .withSSES3(new SSES3());
        S3BucketDestination s3BucketDestination = new S3BucketDestination()
                .withAccountId(exportAccountId)
                .withArn(exportBucketArn)
                .withEncryption(exportEncryption)
                .withFormat(exportFormat)
                .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                .withPrefix("Prefix");
        CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                .withIsEnabled(true);
        StorageLensDataExport dataExport = new StorageLensDataExport()
                .withCloudWatchMetrics(cloudWatchMetrics)
                .withS3BucketDestination(s3BucketDestination);

        StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                .withArn(awsOrgARN);

        StorageLensConfiguration configuration = new StorageLensConfiguration()
                .withId(configurationId)
                .withAccountLevel(accountLevel)
                .withInclude(include)
                .withDataExport(dataExport)
                .withAwsOrg(awsOrg)
                .withIsEnabled(true);

        List<StorageLensTag> tags = Arrays.asList(
                new StorageLensTag().withKey("key-1").withValue("value-1"),
                new StorageLensTag().withKey("key-2").withValue("value-2")
        );

        AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();
```

```
            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Pour améliorer la visibilité de votre stockage, vous pouvez créer un ou plusieurs groupes S3 Storage Lens et les attacher à votre tableau de bord. Un groupe S3 Storage Lens est un filtre défini personnalisé pour les objets basé sur les préfixes, les suffixes, les balises d'objet, la taille d'objet, l'âge d'objet ou une combinaison de ces filtres.

Vous pouvez utiliser les groupes S3 Storage Lens pour obtenir une visibilité précise sur les compartiments partagés de grande taille, tels que les lacs de données, afin de prendre des décisions commerciales plus éclairées. Par exemple, vous pouvez rationaliser l'allocation du stockage et optimiser les rapports sur les coûts en répartissant l'utilisation du stockage en groupes d'objets spécifiques pour des projets individuels et des centres de coûts au sein d'un compartiment ou de plusieurs compartiments.

Pour utiliser les groupes S3 Storage Lens, vous devez mettre à niveau votre tableau de bord afin d'utiliser des métriques et des recommandations avancées. Pour plus d'informations sur les groupes S3 Storage Lens, consultez the section called "Utilisation des groupes Storage Lens".

Mise à jour d'un tableau de bord Amazon S3 Storage Lens

Le tableau de bord par défaut d'Amazon S3 Storage Lens est `default-account-dashboard`. Ce tableau de bord est préconfiguré par Amazon S3 pour vous aider à visualiser le résumé des informations et des tendances des métriques gratuites et avancées agrégées de votre compte

dans la console. Vous ne pouvez pas modifier la portée de la configuration du tableau de bord par défaut, mais vous pouvez mettre à niveau la sélection de métriques gratuites vers les métriques et recommandations avancées payantes, configurer l'exportation facultative des métriques ou même désactiver le tableau de bord par défaut. Ce tableau de bord par défaut ne peut pas être supprimé et peut uniquement être désactivé. Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

Utilisation de la console S3

Suivez les étapes suivantes pour mettre à jour un tableau de bord Amazon S3 Storage Lens sur la console Amazon S3.

Étape 1 : mettre à jour la portée du tableau de bord

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Storage Lens, Tableaux de bord.
3. Choisissez le tableau de bord que vous souhaitez modifier, puis choisissez Edit (Modifier).

   La page Edit dashboard (Modifier le tableau de bord) s'ouvre.

   > **Note**
   >
   > Vous ne pouvez pas modifier les éléments suivants :
   >
   > - Le nom du tableau de bord
   > - La Région d'accueil
   > - La portée de tableau de bord du tableau de bord par défaut, qui est étendue à l'ensemble du stockage de votre compte.

4. (Facultatif) Sur la page de configuration du tableau de bord, dans la section General (Général), mettez à jour et ajoutez des étiquettes dans votre tableau de bord.

   Vous pouvez utiliser des balises pour gérer les autorisations de votre tableau de bord et pour suivre les coûts liés à S3 Storage Lens. Pour plus d'informations, consultez Contrôle de l'accès à l'aide d'étiquettes de ressources dans le Guide de l'utilisateur IAM et Étiquettes de répartition des coûts générées par AWS dans le Guide de l'utilisateur AWS Billing .

> **Note**
>
> Vous pouvez ajouter jusqu'à 50 balises à votre configuration de tableau de bord.

5. Dans la section Dashboard scope (Portée du tableau de bord), procédez comme suit :

   a. Mettez à jour les Régions et les compartiments que S3 Storage Lens doit inclure ou exclure du tableau de bord.

   > **Note**
   >
   > - Vous pouvez inclure ou exclure des Régions et des compartiments. Cette option est limitée aux Régions uniquement lors de la création de tableaux de bord au niveau de l'organisation sur les comptes membres de votre organisation.
   > - Vous pouvez choisir jusqu'à 50 compartiments à inclure ou exclure.

   b. Mettez à jour les compartiments des Régions sélectionnées que vous souhaitez inclure ou exclure de S3 Storage Lens. Vous pouvez inclure ou exclure des compartiments, mais pas les deux. Cette option n'est pas disponible lors de la création de tableaux de bord au niveau de l'organisation.

Étape 2 : mettre à jour la sélection de métriques

1. Dans la section Metrics selection (Sélection de métriques), sélectionnez le type de métriques que vous souhaitez agréger pour ce tableau de bord.

   - Pour inclure des métriques gratuites agrégées au niveau du compartiment et disponibles pour les requêtes pendant 14 jours, choisissez Free Metrics (Métriques gratuites).
   - Pour activer les métriques avancées et d'autres options avancées, choisissez Advanced metrics and recommendations (Métriques et recommandations avancées). Ces options incluent l'agrégation avancée des préfixes, la CloudWatch publication sur Amazon et les recommandations contextuelles. Les données sont disponibles pour les requêtes pendant 15 mois. Les métriques et recommandations avancées entraînent un coût supplémentaire. Pour plus d'informations, consultez Tarification Amazon S3.

     Pour plus d'informations sur les métriques gratuites et avancées, consultez Sélection des métriques.

2. Sous Advanced metrics and recommendations features (Fonctionnalités de métriques et recommandations avancées), sélectionnez les options que vous voulez activer :

   - Advanced metrics (Métriques avancées)
   - CloudWatch publiant
   - Prefix aggregation (Agrégation de préfixes)

   > **Important**
   >
   > Si vous activez l'agrégation de préfixes pour votre configuration S3 Storage Lens, les métriques au niveau du préfixe ne seront pas publiées sur. CloudWatch Seules les métriques S3 Storage Lens au niveau du bucket, du compte et de l'organisation sont publiées sur. CloudWatch

3. Si vous avez activé Advanced metrics (Métriques avancées), sélectionnez les Advanced metrics categories (Catégories de métriques avancées) que vous souhaitez afficher dans votre tableau de bord S3 Storage Lens :

   - Métriques d'activité
   - Detailed status code metrics (Métriques détaillées sur le code de statut)
   - Advanced cost optimization metrics (Métriques avancées sur l'optimisation des coûts)
   - Advanced data protection metrics (Métriques avancées sur la protection des données)

   Pour plus d'informations sur les catégories de métriques, consultez Catégories de métriques. Pour obtenir une liste complète des métriques, consultez Glossaire des métriques Amazon S3 Storage Lens.

4. Si vous avez choisi d'activer l'agrégation des préfixes, configurez les éléments suivants :

   a. Choisissez la taille minimale du seuil de préfixe pour ce tableau de bord.

      Par exemple, un seuil de préfixe de 5 % indique que les préfixes représentant 5 % ou plus de la taille totale de stockage du compartiment seront agrégés.

   b. Sélectionnez la profondeur de préfixe.

      Ce paramètre indique le nombre maximal de niveaux jusqu'auquel les préfixes sont évalués. La profondeur de préfixe doit être inférieure à 10.

c. Saisissez un caractère de délimiteur de préfixe.

Il s'agit de la valeur utilisée pour identifier chaque niveau de préfixe. La valeur par défaut dans Amazon S3 est le caractère `/`, mais votre structure de stockage peut utiliser d'autres délimiteurs.

(Facultatif) Étape 3 : exporter des métriques pour le tableau de bord

1. Dans la section Metrics export (Exportation de métriques), choisissez Enable (Activer) pour créer une exportation de métriques qui sera placée quotidiennement dans un compartiment de destination de votre choix. Pour désactiver l'exportation des métriques, choisissez Disable (Désactiver).

   L'exportation des métriques est au format CSV ou Apache Parquet. La portée des données est la même que celle des données de votre tableau de bord S3 Storage Lens sans les recommandations.

2. Si cette option est activée, choisissez le format de sortie de votre exportation quotidienne de métriques : CSV ou Apache Parquet.

   Parquet est un format de fichier open source pour Hadoop, qui stocke les données imbriquées dans un format en colonnes plat.

3. Sélectionnez le compartiment S3 de destination pour l'exportation de vos métriques.

   Vous pouvez choisir un compartiment dans le compte actuel du tableau de bord S3 Storage Lens. Vous pouvez également en choisir un autre Compte AWS si vous disposez des autorisations du compartiment de destination et de l'ID de compte du propriétaire du compartiment de destination.

4. Choisissez le compartiment S3 de destination (format : `s3://`*`bucket-name`*`/`*`prefix`*).

   Le compartiment doit être dans la région d'origine de votre tableau de bord S3 Storage Lens. La console S3 vous montre le paramètre Destination bucket permission (Autorisation de compartiment de destination) qui sera ajouté par Amazon S3 à la politique de compartiment de destination. Amazon S3 met à jour la politique de compartiment sur le compartiment de destination pour permettre à S3 de placer des données dans ce compartiment.

5. (Facultatif) Pour activer le chiffrement côté serveur pour l'exportation de vos métriques, choisissez Specify an encryption key (Spécifier une clé de chiffrement). Ensuite, choisissez

le Type de chiffrement : Clés gérées par Amazon S3 (SSE-S3) ou Clé AWS Key Management Service (SSE-KMS).

Vous pouvez choisir entre une clé gérée par Amazon S3 (SSE-S3) et une clé AWS Key Management Service (AWS KMS) (SSE-KMS).

6. (Facultatif) Pour spécifier une AWS KMS clé, vous devez choisir une clé KMS ou saisir une clé Amazon Resource Name (ARN). Sous CléAWS KMS , spécifiez votre clé KMS de l'une des manières suivantes :

   - Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos clés AWS KMS keys, puis sélectionnez votre Clé KMS dans la liste des clés disponibles.

     La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans cette liste. Pour plus d'informations sur les clés gérées par le client, consultez Clés de client et clés AWS dans le Guide du développeur AWS Key Management Service .

     > **Note**
     >
     > Le Clé gérée par AWS (`aws/S3`) n'est pas pris en charge pour le chiffrement SSE-KMS avec S3 Storage Lens.

   - Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis entrez l'ARN de votre clé KMS dans le champ qui apparaît.
   - Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

     Si vous choisissez une clé gérée par le client, vous devez accorder à S3 Storage Lens l'autorisation de chiffrer dans la politique de clé AWS KMS . Pour de plus amples informations, veuillez consulter Utilisation d'un AWS KMS key pour chiffrer vos exportations de métriques.

     Pour plus d'informations sur la création d'un AWS KMS key, consultez la section Création de clés dans le guide du AWS Key Management Service développeur.

7. Sélectionnez Enregistrer les modifications.

Pour améliorer la visibilité de votre stockage, vous pouvez créer un ou plusieurs groupes S3 Storage Lens et les attacher à votre tableau de bord. Un groupe S3 Storage Lens est un filtre défini personnalisé pour les objets basé sur les préfixes, les suffixes, les balises d'objet, la taille d'objet, l'âge d'objet ou une combinaison de ces filtres.

Vous pouvez utiliser les groupes S3 Storage Lens pour obtenir une visibilité précise sur les compartiments partagés de grande taille, tels que les lacs de données, afin de prendre des décisions commerciales plus éclairées. Par exemple, vous pouvez rationaliser l'allocation du stockage et optimiser les rapports sur les coûts en répartissant l'utilisation du stockage en groupes d'objets spécifiques pour des projets individuels et des centres de coûts au sein d'un compartiment ou de plusieurs compartiments.

Pour utiliser les groupes S3 Storage Lens, vous devez mettre à niveau votre tableau de bord afin d'utiliser des métriques et des recommandations avancées. Pour plus d'informations sur les groupes S3 Storage Lens, consultez the section called "Utilisation des groupes Storage Lens".

À l'aide du AWS CLI

Example

L'exemple de commande suivant met à jour la configuration d'un tableau de bord Amazon S3 Storage Lens. Pour utiliser ces exemples, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control put-storage-lens-configuration --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --storage-lens-
configuration=file://./config.json --tags=file://./tags.json
```

Utilisation du AWS SDK pour Java

Example – Mettre à jour la configuration par défaut Amazon S3 Storage Lens avec les métriques et recommandations avancées

Les exemples suivants montrent comment mettre à jour la configuration S3 Storage Lens par défaut avec les métriques et recommandations avancées dans le kit SDK pour Java :

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.Format;
```

```
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class UpdateDefaultConfigWithPaidFeatures {

    public static void main(String[] args) {
        String configurationId = "default-account-dashboard"; // This configuration ID
 cannot be modified.
        String sourceAccountId = "111122223333";

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
```

```
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );

        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

> **Note**
>
> Des frais supplémentaires s'appliquent pour les métriques et recommandations avancées. Pour plus d'informations, consultez Métriques et recommandations avancées.

Désactivation d'un tableau de bord Amazon S3 Storage Lens

Vous pouvez désactiver un tableau de bord Amazon S3 Storage Lens à partir de la console Amazon S3. Lorsqu'un tableau de bord est désactivé, il ne peut plus générer de métriques. Un tableau de bord désactivé conserve toujours ses informations de configuration. Ainsi, vous pouvez facilement le reprendre lorsque vous le réactivez. Un tableau de bord désactivé retient ses données historiques jusqu'à ce qu'il ne soit plus disponible pour les requêtes.

Utilisation de la console S3

Suivez la procédure ci-dessous pour créer un tableau de bord Amazon S3 Storage Lens dans la console Amazon S3.

Pour désactiver un tableau de bord Amazon S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux), sélectionnez le tableau de bord que vous souhaitez désactiver, puis sélectionnez Disable (Désactiver) en haut de la liste.
4. Sur la page de confirmation, confirmez que vous souhaitez désactiver le tableau de bord en saisissant son nom dans le champ de texte, puis sélectionnez Confirmer.

Suppression d'un tableau de bord Amazon S3 Storage Lens

Vous ne pouvez pas supprimer le tableau de bord par défaut. Cependant, vous pouvez la ou le désactiver. Avant de supprimer un tableau de bord que vous avez créé, tenez compte des points suivants :

- Au lieu de supprimer un tableau de bord, vous pouvez le désactiver afin qu'il puisse être réactivé à l'avenir. Pour de plus amples informations, veuillez consulter Utilisation de la console S3.
- Lorsque le tableau de bord est supprimé, tous les paramètres de configuration qui lui sont associés sont également supprimés.
- En outre, toutes les données historiques des métriques ne sont plus disponibles. Ces données historiques sont conservées pendant 15 mois. Si vous souhaitez accéder à nouveau à ces données, vous devez créer un tableau de bord portant le même nom dans la même Région d'accueil que celui qui a été supprimé.

Utilisation de la console S3

Vous pouvez supprimer un tableau de bord Amazon S3 Storage Lens à partir de la console Amazon S3. Cependant, lorsqu'un tableau de bord est supprimé, il ne peut plus générer de métriques.

Supprimer un tableau de bord Amazon S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord à supprimer, puis Delete (Supprimer) en haut de la liste.
4. Sur la page Supprimer les tableaux de bord, confirmez que vous souhaitez supprimer le tableau de bord en saisissant son nom dans le champ de texte. Ensuite, choisissez Valider.

En utilisant le AWS CLI

Example

L'exemple suivant supprime une configuration S3 Storage Lens. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

```
aws s3control delete-storage-lens-configuration --account-id=222222222222 --region=us-east-1 --config-id=your-configuration-id
```

Utilisation du AWS SDK pour Java

Example – Supprimer une configuration de tableau de bord Amazon S3 Storage Lens

L'exemple suivant illustre comment supprimer une configuration S3 Storage Lens à l'aide du kit SDK for Java :

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;
```

```
public class DeleteDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.deleteStorageLensConfiguration(new
 DeleteStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Affichage des tableaux de bord Amazon S3 Storage Lens

Utilisation de la console S3

Pour afficher les tableaux de bord S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Choisissez Tableaux de bord. Vous pouvez désormais consulter les tableaux de bord dans votre Compte AWS.

En utilisant le AWS CLI

Example

L'exemple de commande suivant répertorie les tableaux de bord S3 Storage Lens de votre Compte AWS. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1 --next-token=abcdefghij1234
```

Example

L'exemple suivant répertorie les configurations S3 Storage Lens sans jeton suivant. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

```
aws s3control list-storage-lens-configurations --account-id=222222222222 --region=us-east-1
```

Utilisation du AWS SDK pour Java

Example – Répertorie les configurations de tableau de bord S3 Storage Lens

L'exemple suivant illustre comment répertorier les configurations S3 Storage Lens à l'aide du kit SDK pour Java : Pour utiliser cet exemple, remplacez le *user input placeholders* par vos propres informations. » dans chaque description de l'exemple.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationEntry;
import com.amazonaws.services.s3control.model.ListStorageLensConfigurationsRequest;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;
```

```
public class ListDashboard {

    public static void main(String[] args) {
        String sourceAccountId = "111122223333";
        String nextToken = "nextToken";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<ListStorageLensConfigurationEntry> configurations =
                    s3ControlClient.listStorageLensConfigurations(new
 ListStorageLensConfigurationsRequest()
                            .withAccountId(sourceAccountId)
                            .withNextToken(nextToken)
                    ).getStorageLensConfigurationList();

            System.out.println(configurations.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Affichage des détails d'un tableau de bord Amazon S3 Storage Lens

Vous pouvez consulter un tableau de bord Amazon S3 Storage Lens depuis la console Amazon S3 et le SDK for Java. AWS CLI

Utilisation de la console S3

Pour afficher les détails de configuration d'un tableau de bord S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Choisissez Tableaux de bord.
4. Dans la liste Tableaux de bord, sélectionnez le tableau de bord que vous souhaitez afficher. Vous pouvez désormais afficher les détails de votre tableau de bord Storage Lens.

En utilisant le AWS CLI

Example

L'exemple suivant récupère une configuration S3 Storage Lens afin que vous puissiez consulter les détails de la configuration. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-storage-lens-configuration --account-id=222222222222 --config-
id=your-configuration-id --region=us-east-1
```

Utilisation du AWS SDK pour Java

Example — Récupérer et afficher une configuration S3 Storage Lens

L'exemple suivant montre comment récupérer une configuration S3 Storage Lens dans le kit SDK pour Java afin de pouvoir consulter les détails de la configuration. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.GetStorageLensConfigurationResult;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
```

```
        String sourceAccountId = "111122223333";

        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final StorageLensConfiguration configuration =
                    s3ControlClient.getStorageLensConfiguration(new
 GetStorageLensConfigurationRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getStorageLensConfiguration();

            System.out.println(configuration.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Gestion des balises de AWS ressources avec S3 Storage Lens

Chaque tableau de bord Amazon S3 Storage Lens est considéré comme une AWS ressource dotée de son propre Amazon Resource Name (ARN). Par conséquent, lorsque vous configurez votre tableau de bord Storage Lens, vous pouvez éventuellement y ajouter AWS des balises de ressources. Vous pouvez ajouter jusqu'à 50 balises par tableau de bord Storage Lens. Pour créer un tableau de bord Storage Lens avec des balises, vous devez disposer des autorisations S3 Storage Lenssuivantes :

- `s3:ListStorageLensConfigurations`
- `s3:GetStorageLensConfiguration`
- `s3:GetStorageLensConfigurationTagging`
- `s3:PutStorageLensConfiguration`

- `s3:PutStorageLensConfigurationTagging`

Vous pouvez utiliser AWS des balises de ressources pour classer les ressources par département, secteur d'activité ou projet. Cela est utile lorsque vous avez de nombreuses ressources du même type. En appliquant des balises, vous pouvez rapidement identifier un tableau de bord S3 Storage Lens spécifique en fonction des balises que vous lui avez affectées. Vous pouvez également utiliser des balises pour suivre et répartir les coûts.

En outre, lorsque vous ajoutez une balise de AWS ressource à votre tableau de bord Storage Lens, vous activez le contrôle d'accès basé sur les attributs (ABAC). L'ABAC est une stratégie d'autorisation qui définit les autorisations en fonction d'attributs, tels que des balises. Vous pouvez également utiliser des conditions qui spécifient des balises de ressources dans vos politiques IAM pour contrôler l'accès aux AWS ressources.

Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. En outre, tenez compte des limitations suivantes :

- Les clés de balise et valeurs de balise sont sensibles à la casse.
- Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur.
- Si vous supprimez une ressource, ses balises sont également supprimées.
- N'incluez pas de données privées ou sensibles dans vos balises de AWS ressources.
- Les balises système (dont les clés de balise commencent par `aws:`) ne sont pas prises en charge.
- La longueur de chaque clé de balise ne peut pas dépasser 128 caractères. La longueur de chaque valeur de balise ne peut pas dépasser 256 caractères.

Les exemples suivants montrent comment utiliser les balises de AWS ressources avec le tableau de bord Storage Lens.

Rubriques

- Ajouter AWS des balises de ressources à un tableau de bord Storage Lens
- Récupérer AWS des balises de ressources pour un tableau de bord Storage Lens
- Mise à jour des balises de tableau de bord Storage Lens
- Supprimer AWS des balises de ressources d'un tableau de bord S3 Storage Lens

Ajouter AWS des balises de ressources à un tableau de bord Storage Lens

Les exemples suivants montrent comment ajouter AWS des balises de ressources à un tableau de bord S3 Storage Lens. Vous pouvez ajouter des balises de ressources à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour ajouter AWS des balises de ressources à un tableau de bord Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Choisissez Tableaux de bord.
4. Choisissez la case d'option du tableau de bord Storage Lens que vous souhaitez mettre à jour. Ensuite, choisissez Edit (Modifier).
5. Sous Général, choisissez Ajouter une balise.
6. Sur la page Ajouter une balise, ajoutez la nouvelle paire clé-valeur.

   > **Note**
   >
   > L'ajout d'une nouvelle balise ayant la même clé qu'une balise existante remplace la valeur de balise précédente.

7. (Facultatif) Pour ajouter plusieurs nouvelles balises, choisissez à nouveau Ajouter une balise pour continuer à ajouter de nouvelles entrées. Vous pouvez ajouter jusqu'à 50 balises de AWS ressources à votre tableau de bord Storage Lens.
8. (Facultatif) Si vous souhaitez retirer une entrée récemment ajoutée, choisissez Retirer en regard de la balise que vous souhaitez retirer.
9. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

Example

L'exemple de commande suivant ajoute des balises à une configuration de tableau de bord S3 Storage Lens. Pour utiliser ces exemples, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control put-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

Utilisation du AWS SDK pour Java

L'exemple suivant ajoute des balises à une configuration Amazon S3 Storage Lens dans le kit SDK pour Java. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

Example – Ajouter des balises à une configuration S3 Storage Lens

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();
```

```
            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Récupérer AWS des balises de ressources pour un tableau de bord Storage Lens

Les exemples suivants montrent comment récupérer AWS des balises de ressources pour un tableau de bord S3 Storage Lens. Vous pouvez obtenir des balises de ressources à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour récupérer les balises de AWS ressources d'un tableau de bord Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Choisissez Tableaux de bord.
4. Choisissez la case d'option correspondant à la configuration du tableau de bord Storage Lens que vous souhaitez afficher. Choisissez ensuite Afficher la configuration du tableau de bord.
5. Sous Balises, vérifiez les balises associées au tableau de bord.
6. (Facultatif) Pour ajouter une nouvelle balise, choisissez Modifier. Choisissez ensuite Ajouter une balise. Sur la page Ajouter une balise, ajoutez la nouvelle paire clé-valeur.

> **Note**
>
> L'ajout d'une nouvelle balise ayant la même clé qu'une balise existante remplace la valeur de balise précédente.

7. (Facultatif) Si vous souhaitez retirer une entrée récemment ajoutée, choisissez Retirer en regard de la balise que vous souhaitez retirer.
8. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

Example

L'exemple de commande suivant récupère des balises pour la configuration d'un tableau de bord S3 Storage Lens. Pour utiliser ces exemples, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-storage-lens-configuration-tagging --account-id=222222222222 --
region=us-east-1 --config-id=your-configuration-id --tags=file://./tags.json
```

Utilisation du AWS SDK pour Java

Example – Obtenir des balises pour une configuration de tableau de bord S3 Storage Lens

L'exemple suivant illustre comment récupérer des balises pour la configuration d'un tableau de bord S3 Storage Lens dans le kit SDK pour Java. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationRequest;
import
 com.amazonaws.services.s3control.model.GetStorageLensConfigurationTaggingRequest;
```

```
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class GetDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            final List<StorageLensTag> s3Tags = s3ControlClient
                    .getStorageLensConfigurationTagging(new
 GetStorageLensConfigurationTaggingRequest()
                            .withAccountId(sourceAccountId)
                            .withConfigId(configurationId)
                    ).getTags();

            System.out.println(s3Tags.toString());
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Mise à jour des balises de tableau de bord Storage Lens

Les exemples suivants montrent comment mettre à jour les balises du tableau de bord Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour mettre à jour une balise de AWS ressource pour un tableau de bord Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Choisissez Tableaux de bord.
4. Choisissez la case d'option correspondant à la configuration du tableau de bord Storage Lens que vous souhaitez afficher. Choisissez ensuite Afficher la configuration du tableau de bord.
5. Sous Balises, vérifiez les balises associées au tableau de bord.
6. (Facultatif) Pour ajouter une nouvelle balise, choisissez Modifier. Choisissez ensuite Ajouter une balise. Sur la page Ajouter une balise, ajoutez la nouvelle paire clé-valeur.

   > **Note**
   >
   > L'ajout d'une nouvelle balise ayant la même clé qu'une balise existante remplace la valeur de balise précédente.

7. (Facultatif) Si vous souhaitez retirer une entrée récemment ajoutée, choisissez Retirer en regard de la balise que vous souhaitez retirer.
8. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

Example

L'exemple de commande suivant ajoute ou remplace des balises au niveau d'une configuration existante de tableau de bord Amazon S3 Storage Lens. Pour utiliser ces exemples, remplacez *`user input placeholders`* par vos propres informations.

```
aws s3control put-storage-lens-configuration-tagging --account-id=111122223333 --
config-id=example-dashboard-configuration-id --region=us-east-1 --config-id=your-
configuration-id
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant met à jour les balises de AWS ressources d'un tableau de bord Storage Lens existant. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

Example — Mettre à jour les balises au niveau une configuration existante de tableau de bord Storage Lens

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.PutStorageLensConfigurationTaggingRequest;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class PutDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            List<StorageLensTag> tags = Arrays.asList(
                    new StorageLensTag().withKey("key-1").withValue("value-1"),
                    new StorageLensTag().withKey("key-2").withValue("value-2")
            );

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();
```

```
            s3ControlClient.putStorageLensConfigurationTagging(new
 PutStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withTags(tags)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Supprimer AWS des balises de ressources d'un tableau de bord S3 Storage Lens

Les exemples suivants montrent comment supprimer AWS des balises de ressources d'un tableau de bord Storage Lens existant. Vous pouvez supprimer des balises à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour supprimer les balises de AWS ressources d'un tableau de bord Storage Lens existant

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Choisissez Tableaux de bord.
4. Choisissez la case d'option correspondant à la configuration du tableau de bord Storage Lens que vous souhaitez afficher. Choisissez ensuite Afficher la configuration du tableau de bord.
5. Sous Balises, vérifiez les balises associées au tableau de bord.
6. Sélectionnez Supprimer à côté de la balise que vous souhaitez supprimer.
7. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

La AWS CLI commande suivante supprime les balises de AWS ressources d'un tableau de bord Storage Lens existant. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

Example

```
aws s3control delete-storage-lens-configuration-tagging --account-id=222222222222 --
config-id=your-configuration-id --region=us-east-1
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant supprime une balise de AWS ressource du tableau de bord de Storage Lens à l'aide de l'Amazon Resource Name (ARN) que vous spécifiez dans le compte*111122223333*. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

Example – Supprimer des balises pour une configuration de tableau de bord S3 Storage Lens

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import
 com.amazonaws.services.s3control.model.DeleteStorageLensConfigurationTaggingRequest;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class DeleteDashboardTagging {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "111122223333";
        try {
            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();
```

```
            s3ControlClient.deleteStorageLensConfigurationTagging(new
 DeleteStorageLensConfigurationTaggingRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Fichiers d'aide pour l'utilisation d'Amazon S3 Storage Lens

Utilisez les fichiers JSON suivants et ses entrées de clé pour vos exemples.

Exemple de configuration S3 Storage Lens dans JSON

Example **`config.json`**

Le fichier `config.json` contient les détails d'une configuration de métriques et recommandations avancées S3 Storage Lens au niveau de l'organisation. Pour utiliser l'exemple suivant, remplacez *`user input placeholders`* par vos propres informations.

> **Note**
>
> Des frais supplémentaires s'appliquent pour les métriques et recommandations avancées. Pour plus d'informations, consultez Métriques et recommandations avancées.

```
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for AWS Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
```

```
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true
      },
      "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
      },
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true,
          "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
    "Buckets": [ //This attribute is not supported for AWS Organizations-level
configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket"
```

```
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
      "AccountId": "111122223333",
      "Arn": "arn:aws:s3:::
amzn-s3-demo-destination-bucket", // The destination bucket for your metrics export
 must be in the same Region as your S3 Storage Lens configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true
    }
  }
}
```

Exemple de configuration S3 Storage Lens avec des groupes Storage Lens dans JSON

Example **`config.json`**

Le fichier `config.json` contient les détails que vous souhaitez appliquer à votre configuration Storage Lens lorsque vous utilisez des groupes Storage Lens. Pour utiliser l'exemple, remplacez *`user input placeholders`* par vos propres informations.

Pour attacher tous les groupes Storage Lens à votre tableau de bord, mettez à jour votre configuration Storage Lens avec la syntaxe suivante :

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
```

```
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
    "StorageLensGroupLevel": {},
  "IsEnabled": true
}
```

Pour inclure uniquement deux groupes Storage Lens dans la configuration de votre tableau de bord Storage Lens (*slg-1*et*slg-2*), utilisez la syntaxe suivante :

```
{
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Include": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
    },
  "IsEnabled": true
}
```

Pour exclure uniquement certains groupes Storage Lens de la configuration de votre tableau de bord, utilisez la syntaxe suivante :

```
{
```

```
  "Id": "ExampleS3StorageLensConfiguration",
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
      "IsEnabled":true
      },
   "StorageLensGroupLevel": {
        "SelectionCriteria": {
            "Exclude": [
                "arn:aws:s3:us-east-1:111122223333:storage-lens-group/slg-1",
                "arn:aws:s3:us-east-1:444455556666:storage-lens-group/slg-2"
            ]
    },
  "IsEnabled": true
}
```

Exemple de configuration de balises S3 Storage Lens dans JSON

Example **`tags.json`**

Le fichier `tags.json` contient les étiquettes que vous souhaitez appliquer à votre configuration S3 Storage Lens. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
[
    {
        "Key": "key1",
        "Value": "value1"
    },
    {
        "Key": "key2",
        "Value": "value2"
    }
]
```

Exemple de configuration d'autorisations IAM pour S3 Storage Lens

Example **`permissions.json`** : nom de tableau de bord spécifique

Cet exemple de politique montre un fichier `permissions.json` IAM de S3 Storage Lens avec un nom de tableau de bord spécifique spécifié. Remplacez *`value1`*, *`us-east-1`*, *`your-dashboard-name`* et *`example-account-id`* par vos propres valeurs.

JSON

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens/your-dashboard-name"
        }
    ]
}
```

Example **`permissions.json`** : aucun nom de tableau de bord spécifique

Cet exemple de politique montre un fichier `permissions.json` IAM de S3 Storage Lens sans nom de tableau de bord spécifique spécifié. Remplacez *`value1`*, *`us-east-1`* et *`example-account-id`* par vos propres valeurs.

JSON

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:GetStorageLensConfiguration",
                "s3:DeleteStorageLensConfiguration",
                "s3:PutStorageLensConfiguration"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/key1": "value1"
                }
            },
            "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens/*"
        }
    ]
}
```

Affichage des métriques avec Amazon S3 Storage Lens

S3 Storage Lens regroupe vos métriques et affiche les informations dans la section Account snapshot (Instantané du compte) sur la page Buckets (Compartiments) de la console Amazon S3. S3 Storage Lens fournit également un tableau de bord interactif que vous pouvez utiliser pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord dispose d'options d'exploration pour générer et visualiser des informations au niveau de l'organisation, du compte, de la Région AWS, de la classe de stockage, du compartiment, du préfixe ou du groupe Storage Lens. Vous pouvez également envoyer une exportation de métriques quotidienne au format CSV ou Parquet vers un compartiment S3.

Par défaut, tous les tableaux de bord sont configurés avec les métriques gratuites, qui incluent les métriques que vous pouvez utiliser pour comprendre l'utilisation et l'activité sur votre espace de stockage S3, optimiser vos coûts de stockage et mettre en œuvre les bonnes pratiques de protection des données et de gestion des accès. Les métriques gratuites sont agrégées jusqu'au niveau du compartiment. Avec les métriques gratuites, les données sont disponibles pour les requêtes jusqu'à 14 jours.

Les métriques et recommandations avancées incluent les fonctionnalités supplémentaires suivantes que vous pouvez utiliser pour mieux comprendre l'utilisation et l'activité de votre stockage, ainsi que les bonnes pratiques visant à optimiser votre stockage :

- Recommandations contextuelles (disponibles uniquement dans le tableau de bord)
- Métriques avancées (y compris les métriques d'activité agrégées par compartiment)
- Prefix aggregation (Agrégation de préfixes)
- Regroupement des groupes Storage Lens
- Regroupement des groupes Storage Lens
- CloudWatch Publication sur Amazon

Les métriques avancées sont disponibles pour les requêtes pendant 15 mois. L'utilisation de S3 Storage Lens avec des métriques avancées entraîne des frais supplémentaires. Pour de plus amples informations, veuillez consulter Tarification Amazon S3. Pour plus d'informations sur les métriques gratuites et avancées, consultez Sélection des métriques.

Rubriques

- Afficher les métriques S3 Storage Lens sur les tableaux de bord
- Afficher les métriques Amazon S3 Storage Lens à l'aide d'une exportation de données
- Surveillez les métriques de S3 Storage Lens dans CloudWatch
- Cas d'utilisation des métriques Amazon S3 Storage Lens

Afficher les métriques S3 Storage Lens sur les tableaux de bord

Dans la console Amazon S3, S3 Storage Lens fournit un tableau de bord interactif par défaut qui permet de visualiser les informations et les tendances de vos données. Vous pouvez également utiliser ce tableau de bord pour signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protection des données. Votre tableau de bord dispose d'options d'exploration pour générer des informations au niveau du compte, du compartiment, de la Région AWS, du préfixe ou du groupe Storage Lens. Si vous avez activé S3 Storage Lens pour fonctionner AWS Organizations, vous pouvez également générer des informations au niveau de l'organisation (telles que des données pour tous les comptes qui font partie de votre AWS Organizations hiérarchie). Le tableau de bord se charge toujours à la date la plus récente pour laquelle des métriques sont disponibles.

Le tableau de bord par défaut de S3 Storage Lens sur la console est nommé default-account-dashboard. Amazon S3 préconfigure ce tableau de bord pour qu'il affiche le résumé des informations et des tendances pour l'ensemble de votre compte, et les met à jour quotidiennement dans la console S3. Vous ne pouvez pas modifier la portée de la configuration du tableau de bord par défaut, mais vous pouvez mettre à niveau la sélection en passant des métriques gratuites aux métriques et recommandations avancées payantes. Les métriques et recommandations avancées vous donnent accès à des métriques et à des fonctionnalités supplémentaires. Ces fonctionnalités incluent les catégories de mesures avancées, l'agrégation au niveau des préfixes, les recommandations contextuelles et la publication sur Amazon. CloudWatch

Vous pouvez désactiver le tableau de bord par défaut, mais pas le supprimer. Si vous désactivez le tableau de bord par défaut, il n'est plus mis à jour. De plus, vous ne recevrez plus de nouvelles métriques quotidiennes dans S3 Storage Lens ou dans la section Instantané de compte sur la page Compartiments. Vous pourrez toujours voir les données d'historique dans le tableau de bord par défaut jusqu'à l'expiration du délai de 14 jours pour les requêtes de données. Cette période est de 15 mois si vous avez activé les métriques et recommandations avancées. Pour accéder à ces données, vous pouvez réactiver le tableau de bord par défaut pendant la période d'expiration.

Vous pouvez créer des tableaux de bord S3 Storage Lens supplémentaires et les définir en Régions AWS fonction de compartiments ou de comptes S3. Vous pouvez également définir vos tableaux de bord par organisation si vous avez activé l'utilisation de Storage Lens. AWS Organizations Lorsque vous créez ou modifiez un tableau de bord S3 Storage Lens, vous définissez la portée de ce tableau de bord et la sélection des métriques.

Vous pouvez désactiver ou supprimer tous les tableaux de bord supplémentaires que vous créez.

- Si vous désactivez un tableau de bord, il ne sera plus mis à jour et vous ne recevrez plus de nouvelles métriques quotidiennes. Vous pouvez encore voir les données d'historique des métriques gratuites pendant la période d'expiration de 14 jours. Si vous avez activé les métriques et recommandations avancées pour ce tableau de bord, cette période est de 15 mois. Pour accéder à ces données, vous pouvez réactiver le tableau de bord pendant la période d'expiration.
- Si vous supprimez votre tableau de bord, vous perdrez tous ses paramètres de configuration. Vous ne recevrez plus de nouvelles métriques quotidiennes et vous perdrez également l'accès aux données historiques associées à ce tableau de bord. Si vous souhaitez accéder aux données historiques d'un tableau de bord supprimé, vous devez créer un autre tableau de bord portant le même nom dans la même Région d'accueil.

Rubriques

- Afficher un tableau de bord Amazon S3 Storage Lens
- Comprendre votre tableau de bord S3 Storage Lens

Afficher un tableau de bord Amazon S3 Storage Lens

La procédure suivante montre comment afficher un tableau de bord S3 Storage Lens dans la console S3. Pour accéder à des procédures pas à pas basées sur des cas d'utilisation qui montrent comment utiliser votre tableau de bord pour optimiser les coûts, mettre en œuvre les bonnes pratiques et améliorer les performances des applications qui accèdent à vos compartiments S3, consultez Cas d'utilisation des métriques Amazon S3 Storage Lens.

> **Note**
>
> Vous ne pouvez pas utiliser les informations d'identification de l'utilisateur root de votre compte pour afficher les tableaux de bord Amazon S3 Storage Lens. Pour accéder aux tableaux de bord de S3 Storage Lens, vous devez accorder les autorisations requises AWS Identity and Access Management (IAM) à un utilisateur IAM nouveau ou existant. Connectez-vous ensuite à l'aide de ces informations d'identification utilisateur pour accéder aux tableaux de bord S3 Storage Lens. Pour plus d'informations, consultez Définition d'autorisations Amazon S3 Storage Lens et les Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.

   Votre tableau de bord s'ouvre dans S3 Storage Lens. La section Snapshot for date (Instantané pour date) affiche la date la plus récente pour laquelle S3 Storage Lens a collecté des métriques. Votre tableau de bord charge toujours la date la plus récente pour laquelle des métriques sont disponibles.
4. (Facultatif) Pour modifier la date de votre tableau de bord S3 Storage Lens, choisissez une nouvelle date dans le sélecteur de date en haut à droite.

5. (Facultatif) Pour appliquer des filtres temporaires afin de limiter davantage la portée de vos données de tableau de bord, procédez comme suit :

   a. Développez la section Filtres.

   b. Pour filtrer en fonction de comptes Régions AWS, de classes de stockage, de compartiments, de préfixes ou de groupes Storage Lens spécifiques, choisissez les options de filtrage.

   > **Note**
   >
   > Le filtre Préfixes et le filtre Groupes Storage Lens ne peuvent pas être appliqués en même temps.

   c. Pour mettre à jour un filtre, choisissez Apply (Appliquer).

   d. Pour supprimer un filtre, cliquez sur X en regard du filtre.

6. Dans n'importe quelle section de votre tableau de bord S3 Storage Lens, pour voir les données relatives à une métrique spécifique, dans Metric (Métrique), choisissez le nom de la métrique.

7. Dans un graphique ou une visualisation quelconque de votre tableau de bord S3 Storage Lens, vous pouvez explorer des niveaux d'agrégation plus profonds à l'aide des onglets Comptes, Régions AWS, Classes de stockage, Compartiments, Préfixes ou Groupes Storage Lens. Pour obtenir un exemple, consultez Découverte des compartiments Amazon S3 froids.

Comprendre votre tableau de bord S3 Storage Lens

Votre tableau de bord S3 Storage Lens comprend un onglet Overview (Présentation) principal et jusqu'à cinq onglets supplémentaires représentant les différents niveaux d'agrégation :

- Comptes
- Régions AWS
- Classes de stockage
- Compartiments
- Préfixes
- Groupes Storage Lens

Dans l'onglet Overview (Présentation), vos données de tableau de bord sont regroupées en trois sections différentes : Snapshot for date (Instantané pour date), Trends and distributions (Tendances et distributions) et Top N overview (Aperçu des N éléments principaux).

Pour plus d'informations sur votre tableau de bord S3 Storage Lens, consultez les sections suivantes.

Instantané

La section Snapshot for date (Instantané pour date) affiche les métriques récapitulatives que S3 Storage Lens a agrégées pour la date sélectionnée. Ces métriques récapitulatives incluent les métriques suivantes :

- Stockage total : quantité totale de stockage utilisée en octets.
- Nombre d'objets : nombre total d'objets dans votre Compte AWS.
- Taille moyenne d'objet : taille moyenne des objets.
- Compartiments actifs : nombre total de compartiments activement utilisés dont le stockage est supérieur à 0 octet dans votre compte.
- Comptes : nombre de comptes dont le stockage est dans la portée. Cette valeur est 1, sauf si vous utilisez AWS Organizations et que votre S3 Storage Lens dispose d'un accès sécurisé avec un rôle lié à un service valide. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés à un service pour Amazon S3 Storage Lens.
- Compartiments : nombre total de compartiments dans votre compte.

Données des métriques

Pour chaque métrique qui apparaît dans l'instantané, vous pouvez voir les données suivantes :

- Nom de la métrique : nom de la métrique.
- Catégorie de métrique : catégorie dans laquelle la métrique est organisée.
- Total pour date : nombre total pour la date sélectionnée.
- % de variation : pourcentage de variation par rapport à la date du dernier instantané.
- Tendance sur 30 jours : courbe de tendance montrant les variations de la métrique sur une période de 30 jours.
- Recommandation : recommandation contextuelle basée sur les données fournies dans l'instantané. Les recommandations sont disponibles avec les métriques et recommandations avancées. Pour de plus amples informations, veuillez consulter Recommandations.

Catégories de métriques

Vous pouvez éventuellement mettre à jour la section Snapshot for date (Instantané pour date) de votre tableau de bord afin d'afficher les métriques relatives à d'autres catégories. Si vous souhaitez voir des données d'instantané pour des métriques supplémentaires, vous pouvez choisir parmi les Metrics categories (Catégories de métriques) suivantes :

- Optimisation des coûts
- Protection des données
- Activité (disponible avec les métriques avancées)
- Gestion des accès
- Performances
- Événements

La section Snapshot for date (Instantané pour date) affiche uniquement une sélection de métriques pour chaque catégorie. Pour voir toutes les métriques d'une catégorie spécifique, choisissez la métrique dans les sections Trends and distributions (Tendances et distributions) ou Top N overview (Aperçu des N éléments principaux). Pour plus d'informations sur les catégories de métriques, consultez Catégories de métriques. Pour obtenir la liste complète des métriques S3 Storage Lens, consultez Glossaire des métriques Amazon S3 Storage Lens.

Tendances et distributions

La deuxième section de l'onglet Overview (Présentation) est Trends and distributions (Tendances et distributions). Dans la section Trends and distributions (Tendances et distributions), vous pouvez choisir deux métriques à comparer sur une plage de dates que vous définissez. La section Trends and distributions (Tendances et distributions) montre la relation entre deux métriques au fil du temps. Cette section contient des graphiques montrant la distribution Classe de stockage et Région entre les deux tendances que vous suivez. Vous pouvez éventuellement explorer un point de données dans l'un des graphiques pour une analyse approfondie.

Pour une procédure pas à pas utilisant la section Trends and distributions (Tendances et distributions), consultez Identifiez les compartiments qui n'utilisent pas le chiffrement côté serveur AWS KMS pour le chiffrement par défaut (SSE-KMS).

Aperçu des N éléments principaux

La troisième section du tableau de bord S3 Storage Lens est Top N overview (Aperçu des N éléments principaux) (triés par ordre croissant ou décroissant). Cette section affiche les statistiques que vous avez sélectionnées pour le plus grand nombre de comptes, de buckets Régions AWS, de préfixes ou de groupes Storage Lens. Si vous avez activé S3 Storage Lens pour qu'il fonctionne AWS Organizations, vous pouvez également consulter les métriques que vous avez sélectionnées au sein de votre organisation.

Pour une procédure pas à pas utilisant la section Top N overview (Aperçu des N éléments principaux), consultez Identifier vos compartiments S3 les plus importants.

Exploration et analyse par options

Pour vous offrir une expérience d'analyse fluide, le tableau de bord S3 Storage Lens fournit un menu d'actions qui s'affiche lorsque vous choisissez une valeur de graphique quelconque. Pour utiliser ce menu, choisissez une valeur de graphique quelconque pour afficher les valeurs de métriques associées, puis choisissez l'une des deux options suivantes dans la zone qui apparaît :

- L'action Drill down (Explorer) applique la valeur sélectionnée en tant que filtre dans tous les onglets de votre tableau de bord. Vous pouvez ensuite explorer cette valeur pour une analyse plus approfondie.
- L'action Analyser par vous redirige vers l'onglet Dimension que vous sélectionnez et applique cette valeur d'onglet en tant que filtre. Ces onglets incluent Comptes, Régions AWS, Classes de stockage, Compartiments, Préfixes (pour les tableaux de bord où Métriques avancées et Regroupement des préfixes sont activés) et Groupes Storage Lens (pour les tableaux de bord où Métriques avancées et Regroupement des groupes Storage Lens sont activés). Analyser par vous permet de visualiser les données dans le contexte de la nouvelle dimension pour une analyse approfondie.

Les actions Approfondir et Analyser par peuvent être désactivées en cas de résultats illogiques ou dépourvus de valeur. Les actions Approfondir et Analyser par appliquent des filtres en plus de tous les filtres existants dans tous les onglets du tableau de bord. Vous pouvez également supprimer les filtres si nécessaire.

Onglets

Les onglets de niveau de dimension fournissent une vue détaillée de toutes les valeurs au sein d'une dimension particulière. Par exemple, l'onglet Régions AWS affiche les métriques de toutes les

Régions AWS et l'onglet Compartiment affiche les métriques de tous les compartiments. Chaque onglet de dimension contient une mise en page identique composée de quatre sections :

- Un graphique de tendances qui affiche les N premiers éléments de la dimension au cours des 30 derniers jours pour la métrique sélectionnée. Par défaut, ce graphique affiche les 10 premiers éléments, mais vous pouvez réduire ce nombre à 3 éléments ou l'augmenter jusqu'à 50.
- Un histogramme qui présente un graphique à barres verticales pour la date et la métrique sélectionnées. Si vous avez un grand nombre d'éléments à afficher dans ce graphique, vous devrez peut-être le faire défiler horizontalement.
- Un graphique d'analyse à bulles qui représente tous les éléments de la dimension. Ce graphique représente la première métrique sur l'axe des X et la deuxième sur l'axe des Y. La troisième métrique est représentée par la taille de la bulle.
- Une vue des métriques sous forme de grille qui contient chaque élément de la dimension répertoriés en lignes. Les colonnes représentent chaque métrique disponible, disposées dans des onglets de catégorie de métriques pour faciliter la navigation.

Afficher les métriques Amazon S3 Storage Lens à l'aide d'une exportation de données

Les métriques Amazon S3 Storage Lens sont générées quotidiennement dans des fichiers d'exportation au format CSV ou Apache Parquet et placées dans un compartiment S3 de votre compte. À partir de là, vous pouvez intégrer les statistiques exportées dans les outils d'analyse de votre choix, tels qu'Amazon QuickSight et Amazon Athena, où vous pouvez analyser l'utilisation du stockage et les tendances en matière d'activité.

Rubriques

- Utilisation d'un AWS KMS key pour chiffrer vos exportations de métriques
- Qu'est-ce qu'un manifeste d'exportation S3 Storage Lens ?
- Comprendre le schéma d'exportation d'Amazon S3 Storage Lens

Utilisation d'un AWS KMS key pour chiffrer vos exportations de métriques

Pour accorder à Amazon S3 Storage Lens l'autorisation de chiffrer vos exportations de métriques à l'aide d'une clé gérée par le client, vous devez utiliser une politique de clé. Pour mettre à jour votre politique de clé et pouvoir utiliser une clé KMS permettant de chiffrer vos exportations de métriques S3 Storage Lens, procédez comme suit.

Pour accorder des autorisations S3 Storage Lens afin de chiffrer des données à l'aide de votre clé KMS

1. Connectez-vous au en AWS Management Console utilisant le propriétaire Compte AWS de la clé gérée par le client.
2. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
3. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
4. Dans le panneau de navigation de gauche, choisissez Clés gérées par le client.
5. Sous Clés gérées par le client, choisissez la clé que vous souhaitez utiliser pour chiffrer les exportations de métriques. AWS KMS keys sont spécifiques à une région et doivent se trouver dans la même région que le compartiment S3 de destination d'exportation des métriques.
6. Sous Politique de clé, choisissez Passer à l'écran de la politique.
7. Pour mettre à jour la politique de clé, choisissez Modifier.
8. Sous Modifier la politique de clé, ajoutez la politique de clé suivante à la politique de clé existante. Pour utiliser cette politique, remplacez *user input placeholders* par vos informations.

```
{
    "Sid": "Allow Amazon S3 Storage Lens use of the KMS key",
     "Effect": "Allow",
    "Principal": {
        "Service": "storage-lens.s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition": {
       "StringEquals": {
           "aws:SourceArn": "arn:aws:s3:us-east-1:source-account-id:storage-
lens/your-dashboard-name",
           "aws:SourceAccount": "source-account-id"
        }
     }
}
```

9. Sélectionnez Enregistrer les modifications.

Pour en savoir plus sur la création de clés gérées par le client et l'utilisation des politiques de clés, consultez les rubriques suivantes dans le guide du développeur AWS Key Management Service :

- Premiers pas
- Utilisation de politiques clés dans AWS KMS

Vous pouvez également utiliser l'opération d'API de politique AWS KMS PUT clé (PutKeyPolicy) pour copier la politique clé dans les clés gérées par le client que vous souhaitez utiliser pour chiffrer les exportations de métriques à l'aide de l'API REST AWS CLI, et SDKs.

Qu'est-ce qu'un manifeste d'exportation S3 Storage Lens ?

Compte tenu de la grande quantité de données agrégées, l'exportation quotidienne de métriques S3 Storage Lens peut être divisée en plusieurs fichiers. Le fichier manifeste `manifest.json` décrit où se trouvent les fichiers d'exportation des métriques d'un jour donné. Chaque fois qu'une nouvelle exportation est livrée, elle est accompagnée d'un nouveau manifeste. Chaque manifeste contenu dans le fichier `manifest.json` fournit des métadonnées et d'autres informations de base sur l'exportation.

Les informations du manifeste comprennent les propriétés suivantes :

- `sourceAccountId` — ID de compte du propriétaire de la configuration.
- `configId` — Identifiant unique du tableau de bord.
- `destinationBucket` — Compartiment de destination Amazon Resource Name (ARN) dans lequel l'exportation des métriques est placée.
- `reportVersion` — Version de l'exportation.
- `reportDate` — Date du rapport.
- `reportFormat` — Format du rapport.
- `reportSchema` — Schéma du rapport.
- `reportFiles` — Liste réelle des fichiers de rapport d'exportation qui se trouvent dans le compartiment de destination.

Voici un exemple de manifeste dans un fichier `manifest.json` pour une exportation au format CSV.

```
{
```

```
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"CSV",

 "reportSchema":"version_number,configuration_id,report_date,aws_account_number,aws_region,stor
   "reportFiles":[
        {
            "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-
configuration-id/V_1/reports/dt=2020-11-03/a38f6bc4-2e3d-4355-ac8a-e2fdcf3de158.csv",
            "size":1603959,
            "md5Checksum":"2177e775870def72b8d84febe1ad3574"
        }
      ]
}
```

Voici un exemple de manifeste dans un fichier `manifest.json` pour une exportation au format Parquet.

```
{
   "sourceAccountId":"123456789012",
   "configId":"my-dashboard-configuration-id",
   "destinationBucket":"arn:aws:s3:::amzn-s3-demo-destination-bucket",
   "reportVersion":"V_1",
   "reportDate":"2020-11-03",
   "reportFormat":"Parquet",
   "reportSchema":"message s3.storage.lens { required string version_number;
 required string configuration_id; required string report_date; required string
 aws_account_number; required string aws_region; required string storage_class;
 required string record_type; required string record_value; required string
 bucket_name; required string metric_name; required long metric_value; }",
   "reportFiles":[
      {
         "key":"DestinationPrefix/StorageLens/123456789012/my-dashboard-configuration-
id/V_1/reports/dt=2020-11-03/bd23de7c-b46a-4cf4-bcc5-b21aac5be0f5.par",
         "size":14714,
         "md5Checksum":"b5c741ee0251cd99b90b3e8eff50b944"
      }
}
```

Vous pouvez configurer l'exportation de vos métriques pour qu'elle soit générée dans le cadre de la configuration de votre tableau de bord dans la console Amazon S3 ou à l'aide de l'API REST Amazon S3 AWS CLI, et SDKs.

Comprendre le schéma d'exportation d'Amazon S3 Storage Lens

Le tableau suivant présente le schéma de l'exportation des métriques S3 Storage Lens.

Nom d'attribut	Type de données	Nom de la colonne	Description
`VersionNumber`	Chaîne	`version_number`	Version des métriques de S3 Storage Lens en cours d'utilisation.
`ConfigurationId`	Chaîne	`configuration_id`	`configuration_id` de votre configuration S3 Storage Lens.
`ReportDate`	Chaîne	`report_date`	Date à laquelle les métriques ont été suivies.
`AwsAccountNumber`	Chaîne	`aws_account_number`	Ton Compte AWS numéro.
`AwsRegion`	Chaîne	`aws_region`	Les indicateurs Région AWS pour lesquels les mesures sont suivies.
`StorageClass`	Chaîne	`storage_class`	Classe de stockage du compartiment en question.
`RecordType`	ENUM	`record_type`	Type d'artefact indiqué (ACCOUNT, BUCKET ou PREFIX).

Nom d'attribut	Type de données	Nom de la colonne	Description
`RecordValue`	Chaîne	`record_value`	La valeur de l'artefact `RecordType` . **Note** La valeur `record_value` est codée dans l'URL.
`BucketName`	Chaîne	`bucket_name`	Nom du compartiment indiqué.
`MetricName`	Chaîne	`metric_name`	Nom de la métrique indiquée.
`MetricValue`	Long	`metric_value`	Valeur de la métrique indiquée.

Exemple d'exportation de métriques S3 Storage Lens

Voici un exemple d'exportation de métriques S3 Storage Lens basée sur ce schéma.

Note

Vous pouvez identifier les métriques pour les groupes Storage Lens en recherchant les valeurs `STORAGE_LENS_GROUP_BUCKET` ou `STORAGE_LENS_GROUP_ACCOUNT` ou dans la colonne `record_type`. La colonne `record_value` affichera l'Amazon Resource Name (ARN) du groupe Storage Lens, par exemple `arn:aws:s3:us-east-1:123456789012:storage-lens-group/slg-1`.

version_r	configuration_id	report_date	aws_account_number	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			StorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ReplicatedStorageBytes	20000
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ReplicatedObjectCount	20
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			EncryptedStorageBytes	2478828742
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			EncryptedObjectCount	1598961
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			DeleteMarkerObjectCount	1500
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			CurrentVersionStorageBytes	2478830621
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			CurrentVersionObjectCount	1598962
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	eu-west-1	STANDARD	ACCOUNT			IncompleteMultipartUploadObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	StorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	ObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	ReplicatedStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	ReplicatedObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	EncryptedStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	EncryptedObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	DeleteMarkerObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	ObjectLockEnabledStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	ObjectLockEnabledObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	CurrentVersionStorageBytes	29996800
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	CurrentVersionObjectCount	12264
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	NonCurrentVersionStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	NonCurrentVersionObjectCount	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	IncompleteMultipartUploadStorageBytes	0
V_1	sample-cmh-exclude	11/3/2020	546264889236	us-west-1	STANDARD	PREFIX	AWSLogs%2F546264889236%2FCloudTrail%2Fus	cloudtrail-log-sfo	IncompleteMultipartUploadObjectCount	0

Voici un exemple d'exportation de métriques S3 Storage Lens avec des données de groupes Storage Lens.

version_numbe	configuration_id	report_date	aws_account_num	aws_region	storage_class	record_type	record_value	bucket_name	metric_name	metric_value
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		StorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		EncryptedObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionStorageBytes	3128548856
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		CurrentVersionObjectCount	4440
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedStorageBytesSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_ACCOUNT	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180		IncompleteMPUObjectCountOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	StorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	EncryptedObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ObjectLockEnabledObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionStorageBytes	676863200
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	CurrentVersionObjectCount	3000
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	NonCurrentVersionObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMultipartUploadObjectCount	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	DeleteMarkerStorageBytes	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedStorageBytesSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	ReplicatedObjectCountSource	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMPUStorageBytesOlderThan7Days	0
V_1	sample-sfo-exclude	11/15/23	546264889236	us-west-1	STANDARD	STORAGE_LENS_GROUP_BUCKET	arn:aws:s3:us-west-1:546264889236:storage-lens-group/age-more-than-180	cloud-trail-log-sfo	IncompleteMPUObjectCountOlderThan7Days	0

Surveillez les métriques de S3 Storage Lens dans CloudWatch

Vous pouvez publier les métriques S3 Storage Lens sur Amazon CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatchtableaux de bord. Vous pouvez également utiliser des CloudWatch fonctionnalités, telles que les alarmes et les actions déclenchées, les mathématiques métriques et la détection des anomalies, pour surveiller et agir sur les métriques S3 Storage Lens. En outre, les opérations CloudWatch d'API permettent aux applications, y compris

aux fournisseurs tiers, d'accéder à vos métriques S3 Storage Lens. Pour plus d'informations sur les CloudWatch fonctionnalités, consultez le guide de CloudWatch l'utilisateur Amazon.

Vous pouvez activer l'option de CloudWatch publication pour les configurations de tableau de bord nouvelles ou existantes à l'aide de la console Amazon S3, de l'API REST Amazon S3 et AWS SDKs. AWS CLI Les tableaux de bord mis à niveau vers les métriques et recommandations avancées de S3 Storage Lens peuvent utiliser l'option de CloudWatch publication. Pour obtenir la tarification des métriques et recommandations avancées S3 Storage Lens, consultez Tarification Amazon S3. Aucun frais de publication de CloudWatch statistiques supplémentaires ne s'applique ; toutefois, d'autres CloudWatch frais, tels que les tableaux de bord, les alarmes et les appels d'API, s'appliquent. Pour plus d'informations, consultez les CloudWatchtarifs Amazon.

Les métriques S3 Storage Lens sont publiées sur le compte propriétaire de la configuration S3 Storage Lens. CloudWatch Après avoir activé l'option de CloudWatch publication dans les métriques et recommandations avancées, vous pouvez accéder aux métriques au niveau de l'organisation, du compte et du bucket dans. CloudWatch Les métriques au niveau du préfixe ne sont pas disponibles dans. CloudWatch

> **Note**
>
> Les métriques S3 Storage Lens sont des statistiques quotidiennes publiées CloudWatch une fois par jour. Lorsque vous interrogez les métriques de S3 Storage Lens dans CloudWatch, la période de requête doit être d'un jour (86 400 secondes). Une fois que vos métriques quotidiennes de S3 Storage Lens apparaissent dans votre tableau de bord S3 Storage Lens dans la console Amazon S3, l'affichage de ces mêmes métriques peut prendre quelques heures CloudWatch. Lorsque vous activez l'option de CloudWatch publication pour les métriques S3 Storage Lens pour la première fois, la publication de vos métriques peut prendre jusqu'à 24 heures CloudWatch.

Après avoir activé l'option de CloudWatch publication, vous pouvez utiliser les CloudWatch fonctionnalités suivantes pour surveiller et analyser les données de votre S3 Storage LensStorage Lens :

- Tableaux de bord — Utilisez des CloudWatch tableaux de bord pour créer des tableaux de bord S3 Storage Lens personnalisés. Partagez votre CloudWatch tableau de bord avec des personnes qui n'ont pas un accès direct au vôtre Compte AWS, avec toutes les équipes, avec les parties prenantes et avec des personnes extérieures à vos organisations.

- Alarmes et actions déclenchées : configurez les alarmes qui surveillent les métriques et agissent lorsqu'un seuil est dépassé. Par exemple, vous pouvez configurer une alarme qui envoie une notification Amazon SNS lorsque la métrique Octets de chargements partitionnés non terminés dépasse 1 Go pendant trois jours consécutifs.
- Détection des anomalies : activez la détection des anomalies pour analyser les métriques continuellement, déterminer l'activité normale et les anomalies de surface. Vous pouvez créer une alarme de détection d'anomalie basées sur la valeur attendue d'une métrique. Par exemple, vous pouvez surveiller les anomalies pour la métrique Octets activés par le verrouillage d'objet afin de détecter la suppression non autorisée des paramètres de verrouillage d'objet.
- Mathématiques appliquées aux métriques : vous pouvez également utiliser les mathématiques appliquées aux métriques pour interroger plusieurs métriques S3 Storage Lens et utiliser des expressions mathématiques pour créer des séries temporelles basées sur ces métriques. Par exemple, vous pouvez créer une nouvelle métrique pour obtenir la taille moyenne d'objet en divisant `StorageBytes` par `ObjectCount`.

Pour plus d'informations sur l'option de CloudWatch publication des métriques S3 Storage Lens, consultez les rubriques suivantes.

Rubriques

- Métriques et dimensions S3 Storage Lens
- Activation de la CloudWatch publication pour S3 Storage Lens
- Utilisation des métriques de S3 Storage Lens dans CloudWatch

Métriques et dimensions S3 Storage Lens

Pour envoyer des métriques de S3 Storage Lens à CloudWatch, vous devez activer l'option de CloudWatch publication dans les métriques et recommandations avancées de S3 Storage Lens. Une fois les métriques avancées activées, vous pouvez utiliser CloudWatchdes tableaux de bord pour surveiller les métriques de S3 Storage Lens ainsi que celles d'autres applications et créer une vue unifiée de l'état de vos opérations. Vous pouvez utiliser des dimensions pour filtrer vos métriques S3 Storage Lens CloudWatch par organisation, compte, compartiment, classe de stockage, région et ID de configuration des métriques.

Les métriques S3 Storage Lens sont publiées sur le compte propriétaire de la configuration S3 Storage Lens. CloudWatch Après avoir activé l'option de CloudWatch publication dans les métriques et recommandations avancées, vous pouvez accéder aux métriques au niveau de l'organisation, du

compte et du bucket dans. CloudWatch Les métriques au niveau du préfixe ne sont pas disponibles dans. CloudWatch

> **Note**
>
> Les métriques S3 Storage Lens sont des statistiques quotidiennes publiées CloudWatch une fois par jour. Lorsque vous interrogez les métriques de S3 Storage Lens dans CloudWatch, la période de requête doit être d'un jour (86 400 secondes). Une fois que vos métriques quotidiennes de S3 Storage Lens apparaissent dans votre tableau de bord S3 Storage Lens dans la console Amazon S3, l'affichage de ces mêmes métriques peut prendre quelques heures CloudWatch. Lorsque vous activez l'option de CloudWatch publication pour les métriques S3 Storage Lens pour la première fois, la publication de vos métriques peut prendre jusqu'à 24 heures CloudWatch.

Pour plus d'informations sur les métriques et les dimensions de S3 Storage Lens dans CloudWatch, consultez les rubriques suivantes.

Rubriques

- Métriques
- Dimensions

Métriques

Les métriques S3 Storage Lens sont disponibles sous forme de métriques dans CloudWatch. Les métriques S3 Storage Lens sont publiées sur l'espace de noms `AWS/S3/Storage-Lens`. Cet espace de noms est réservé aux métriques S3 Storage Lens. Les métriques de compartiment, de demande et de réplication Amazon S3 sont publiées sur l'espace de noms `AWS/S3`.

Les métriques S3 Storage Lens sont publiées sur le compte propriétaire de la configuration S3 Storage Lens. CloudWatch Après avoir activé l'option de CloudWatch publication dans les métriques et recommandations avancées, vous pouvez accéder aux métriques au niveau de l'organisation, du compte et du bucket dans. CloudWatch Les métriques au niveau du préfixe ne sont pas disponibles dans. CloudWatch

Dans S3 Storage Lens, les métriques sont agrégées et stockées uniquement dans la Région d'origine désignée. Les métriques de S3 Storage Lens sont également publiées CloudWatch dans la région d'origine que vous spécifiez dans la configuration de S3 Storage Lens.

Pour obtenir la liste complète des métriques S3 Storage Lens, y compris la liste des métriques disponibles dans CloudWatch, voirGlossaire des métriques Amazon S3 Storage Lens.

> **Note**
>
> La statistique valide pour les métriques S3 Storage Lens dans CloudWatch est Average. Pour plus d'informations sur les statistiques dans CloudWatch, consultez les définitions CloudWatch des statistiques dans le guide de CloudWatch l'utilisateur Amazon.

Granularité des métriques de S3 Storage Lens dans CloudWatch

S3 Storage Lens offre des métriques selon une granularité au niveau de l'organisation, du compte, du compartiment et des préfixes. S3 Storage Lens publie les métriques S3 Storage Lens au niveau de l'organisation, du compte et du bucket sur. CloudWatch Les métriques S3 Storage Lens au niveau du préfixe ne sont pas disponibles dans. CloudWatch

Pour plus d'informations sur la granularité des métriques S3 Storage Lens disponibles dans CloudWatch, consultez la liste suivante :

- Organisation : métriques agrégées sur les comptes membres de votre organisation. S3 Storage Lens publie les statistiques relatives aux comptes des membres CloudWatch dans le compte de gestion.
  - Organisation et compte : métriques pour les comptes membres de votre organisation.
  - Organisation et compartiment : métriques pour les compartiments Amazon S3 dans les comptes membres de votre organisation.
- Compte (hors de l'organisation) : mesures agrégées dans les compartiments de votre compte.
- Compartiment (hors de l'organisation) : métriques pour un compartiment spécifique. Dans CloudWatch, S3 Storage Lens publie ces métriques sur le site Compte AWS qui a créé la configuration S3 Storage Lens. S3 Storage Lens publie ces métriques uniquement pour les configurations non organisationnelles.

Dimensions

Lorsque S3 Storage Lens envoie des données à CloudWatch, des dimensions sont associées à chaque métrique. Les dimensions sont des catégories qui décrivent les caractéristiques des métriques. Vous pouvez utiliser des dimensions pour filtrer les résultats CloudWatch renvoyés.

Par exemple, toutes les métriques de S3 Storage Lens CloudWatch contiennent la `configuration_id` dimension. Vous pouvez utiliser cette dimension pour différencier les métriques associées à une configuration spécifique de S3 Storage Lens. La dimension `organization_id` identifie les métriques au niveau de l'organisation. Pour plus d'informations sur les dimensions dans CloudWatch, voir Dimensions dans le guide de CloudWatch l'utilisateur.

Différentes dimensions sont disponibles pour les métriques S3 Storage Lens selon la granularité des métriques. Par exemple, vous pouvez utiliser la `organization_id` dimension pour filtrer les métriques au niveau de l'organisation en fonction de l' AWS Organizations ID. Toutefois, vous ne pouvez pas utiliser cette dimension pour les métriques au niveau du compartiment ni du compte. Pour de plus amples informations, veuillez consulter Filtrage des métriques à l'aide de dimensions.

Pour savoir quelles dimensions sont disponibles pour votre configuration S3 Storage Lens, consultez le tableau suivant.

Dimension	Description	Compartiment	Configuration	Organisation	Organisation et compte	Organisation et compte
`configuration_id`	Nom du tableau de bord pour la configuration S3 Storage Lens indiqué dans les métriques	.	.	.	.	.
`metrics_version`	Version des métriques S3 Storage Lens. La valeur fixe de la version des métriques est égale à `1.0`.	.	.	.	.	.
`organization_id`	L' AWS Organizations identifiant des métriques	.	.	.	.	.
`aws_account_number`	Le Compte AWS qui est associé aux métriques	.	.	.	.	.
`aws_region`	Le Région AWS pour les métriques	.	.	.	.	.
`bucket_name`	Nom du compartiment S3 indiqué dans les métriques	.	.	.	.	.

Dimension	Description	Compartiment	Configuration et compartiment	Organisation et compte	Organisation et compte
`storage_class`	Classe de stockage pour le compartiment indiqué dans les métriques	.	.	.	.
`record_type`	Granularité des métriques : ORGANISATION, COMPTE, COMPARTIMENT	COMPARTIMENT	COMPTE	COMPARTIMENT	ORGANISATION

Activation de la CloudWatch publication pour S3 Storage Lens

Vous pouvez publier les métriques S3 Storage Lens sur Amazon CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatchtableaux de bord. Vous pouvez également utiliser des CloudWatch fonctionnalités, telles que les alarmes et les actions déclenchées, les mathématiques métriques et la détection des anomalies, pour surveiller et agir sur les métriques S3 Storage Lens. En outre, les opérations CloudWatch d'API permettent aux applications, y compris aux fournisseurs tiers, d'accéder à vos métriques S3 Storage Lens. Pour plus d'informations sur les CloudWatch fonctionnalités, consultez le guide de CloudWatch l'utilisateur Amazon.

Les métriques S3 Storage Lens sont publiées sur le compte propriétaire de la configuration S3 Storage Lens. CloudWatch Après avoir activé l'option de CloudWatch publication dans les métriques et recommandations avancées, vous pouvez accéder aux métriques au niveau de l'organisation, du compte et du bucket dans. CloudWatch Les métriques au niveau du préfixe ne sont pas disponibles dans. CloudWatch

Vous pouvez activer la CloudWatch prise en charge de configurations de tableau de bord nouvelles ou existantes à l'aide de la console S3 APIs AWS CLI, Amazon S3 REST et AWS SDKs. L'option de CloudWatch publication est disponible pour les tableaux de bord mis à niveau vers les métriques et recommandations avancées de S3 Storage Lens. Pour obtenir la tarification des métriques et recommandations avancées S3 Storage Lens, consultez Tarification Amazon S3. Aucun frais de publication de CloudWatch statistiques supplémentaires ne s'applique ; toutefois, d'autres CloudWatch frais, tels que les tableaux de bord, les alarmes et les appels d'API, s'appliquent.

Pour activer l'option de CloudWatch publication pour les métriques S3 Storage Lens, consultez les rubriques suivantes.

> **Note**
>
> Les métriques S3 Storage Lens sont des statistiques quotidiennes publiées CloudWatch une fois par jour. Lorsque vous interrogez les métriques de S3 Storage Lens dans CloudWatch, la période de requête doit être d'un jour (86 400 secondes). Une fois que vos métriques quotidiennes de S3 Storage Lens apparaissent dans votre tableau de bord S3 Storage Lens dans la console Amazon S3, l'affichage de ces mêmes métriques peut prendre quelques heures CloudWatch. Lorsque vous activez l'option de CloudWatch publication pour les métriques S3 Storage Lens pour la première fois, la publication de vos métriques peut prendre jusqu'à 24 heures CloudWatch.
> Actuellement, les métriques S3 Storage Lens ne peuvent pas être consommées par le biais de CloudWatch flux.

Utilisation de la console S3

Lorsque vous mettez à jour un tableau de bord S3 Storage Lens, vous ne pouvez pas modifier le nom du tableau de bord ni la région d'origine. Vous ne pouvez pas non plus modifier la portée du tableau de bord par défaut, qui est délimitée à l'ensemble du stockage de votre compte.

Pour mettre à jour un tableau de bord S3 Storage Lens afin d'activer la CloudWatch publication

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez S3 Storage Lens, Tableaux de bord.
3. Choisissez le tableau de bord que vous souhaitez modifier, puis choisissez Edit (Modifier).
4. Sous Metrics selection (Sélection des métriques), choisissez Advanced metrics and recommendations (Métriques et recommandations avancées).

   Des métriques et recommandations avancées sont disponibles moyennant des frais supplémentaires. Les mesures et recommandations avancées incluent une période de 15 mois pour les requêtes de données, les mesures d'utilisation agrégées au niveau du préfixe, les mesures d'activité agrégées par compartiment, l'option de CloudWatch publication et les recommandations contextuelles qui vous aident à optimiser les coûts de stockage et à appliquer

les meilleures pratiques en matière de protection des données. Pour plus d'informations, consultez Tarification Amazon S3.

5. Sous Sélectionner les fonctionnalités avancées de mesures et de recommandations, sélectionnez la CloudWatchpublication.

> **Important**
>
> Si votre configuration active l'agrégation de préfixes pour les métriques d'utilisation, les métriques au niveau du préfixe ne seront pas publiées sur. CloudWatch Seules les métriques S3 Storage Lens au niveau du bucket, du compte et de l'organisation sont publiées sur. CloudWatch

6. Sélectionnez Enregistrer les modifications.

Pour créer un nouveau tableau de bord S3 Storage Lens permettant l' CloudWatchassistance

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Choisissez Create dashboard (Créer un tableau de bord).
4. Sous General (Général), définissez les options de configuration suivantes :

   a. Dans Dashboard name (Nom du tableau de bord), saisissez le nom de votre tableau de bord.

      Les noms de tableau de bord doivent contenir moins de 65 caractères et ne doivent pas contenir de caractères spéciaux ou d'espaces. Vous ne pouvez pas modifier le nom d'un tableau de bord une fois que vous l'avez créé.

   b. Sélectionnez la Région d'origine de votre tableau de bord.

      Les métriques de toutes les Régions incluses dans la portée de ce tableau de bord sont stockées de manière centralisée dans la Région d'origine désignée. Dans CloudWatch, les métriques S3 Storage Lens sont également disponibles dans la région d'origine. Vous ne pouvez pas modifier la région d'origine une fois que vous avez créé votre tableau de bord.

5. (Facultatif) Pour ajouter des étiquettes, choisissez Add tag (Ajouter une balise) et saisissez la Key (Clé) d'étiquette et une Value (Valeur).

> **Note**
>
> Vous pouvez ajouter jusqu'à 50 balises à votre configuration de tableau de bord.

6. Définissez la portée de votre configuration :

   a. Si vous créez une configuration au niveau de l'organisation, choisissez les comptes à inclure dans la configuration : Include all accounts in your configuration (Inclure tous les comptes dans votre configuration) ou Limit the scope to your signed-in account (Limiter la portée au compte connecté).

   > **Note**
   >
   > Lorsque vous créez une configuration au niveau de l'organisation qui inclut tous les comptes, vous pouvez inclure ou exclure uniquement des régions, et non pas des compartiments.

   b. Choisissez les régions et les compartiments que vous souhaitez que S3 Storage Lens inclue de la configuration du tableau de bord en procédant comme suit :

   - Pour inclure toutes les Régions, choisissez Inclure les Régions et les compartiments.
   - Pour inclure des Régions spécifiques, effacez Inclure toutes les Régions. Sous Choisir les Régions à inclure, choisissez les Régions que vous souhaitez que S3 Storage Lens inclue dans le tableau de bord.
   - Pour inclure des compartiments spécifiques, effacez Include all buckets (Inclure tous les compartiments). Sous Choose buckets to include (Choisir les compartiments à inclure), choisissez les compartiments que vous souhaitez que S3 Storage Lens inclue dans le tableau de bord.

   > **Note**
   >
   > Vous pouvez choisir jusqu'à 50 compartiments.

7. Pour Metrics selection (Sélection des métriques), choisissez Advanced metrics and recommendations (Métriques et recommandations avancées).

Pour plus d'informations sur la tarification des métriques et recommandations avancées, consultez Tarification Amazon S3.

8. Sous Advanced metrics and recommendations features (Fonctionnalités de métriques et recommandations avancées), sélectionnez les options que vous voulez activer :

   - Advanced metrics (Métriques avancées)
   - CloudWatch publiant

   > **Important**
   >
   > Si vous activez l'agrégation de préfixes pour votre configuration S3 Storage Lens, les métriques au niveau du préfixe ne seront pas publiées sur. CloudWatch Seules les métriques S3 Storage Lens au niveau du bucket, du compte et de l'organisation sont publiées sur. CloudWatch

   - Prefix aggregation (Agrégation de préfixes)

   > **Note**
   >
   > Pour plus d'informations sur les fonctionnalités des métriques et recommandations avancées, consultez Sélection des métriques.

9. Si vous avez activé Advanced metrics (Métriques avancées), sélectionnez les Advanced metrics categories (Catégories de métriques avancées) que vous souhaitez afficher dans votre tableau de bord S3 Storage Lens :

   - Métriques d'activité
   - Detailed status code metrics (Métriques détaillées sur le code de statut)
   - Advanced cost optimization metrics (Métriques avancées sur l'optimisation des coûts)
   - Advanced data protection metrics (Métriques avancées sur la protection des données)

   Pour plus d'informations sur les catégories de métriques, consultez Catégories de métriques. Pour obtenir une liste complète des métriques, consultez Glossaire des métriques Amazon S3 Storage Lens.

10. (Facultatif) Configurez l'exportation de vos métriques.

Pour plus d'informations sur la configuration d'une exportation de métriques, consultez l'étape Utilisation de la console S3.

11. Choisissez Create dashboard (Créer un tableau de bord).

En utilisant le AWS CLI

L' AWS CLI exemple suivant active l'option de CloudWatch publication en utilisant une configuration de mesures et de recommandations avancées au niveau de l'organisation S3 Storage Lens. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws s3control put-storage-lens-configuration --account-id=555555555555 --config-
id=your-configuration-id --region=us-east-1 --storage-lens-configuration=file://./
config.json

config.json
{
  "Id": "SampleS3StorageLensConfiguration", //Use this property to identify your S3
 Storage Lens configuration.
  "AwsOrg": { //Use this property when enabling S3 Storage Lens for AWS Organizations.
    "Arn": "arn:aws:organizations::123456789012:organization/o-abcdefgh"
  },
  "AccountLevel": {
    "ActivityMetrics": {
      "IsEnabled":true
    },
    "AdvancedCostOptimizationMetrics": {
      "IsEnabled":true
    },
    "AdvancedDataProtectionMetrics": {
      "IsEnabled":true
    },
    "DetailedStatusCodesMetrics": {
      "IsEnabled":true
    },
    "BucketLevel": {
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "ActivityMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
```

```
      "AdvancedCostOptimizationMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "DetailedStatusCodesMetrics": {
        "IsEnabled":true //Mark this as false if you want only free metrics.
      },
      "PrefixLevel":{
        "StorageMetrics":{
          "IsEnabled":true, //Mark this as false if you want only free metrics.
          "SelectionCriteria":{
            "MaxDepth":5,
            "MinStorageBytesPercentage":1.25,
            "Delimiter":"/"
          }
        }
      }
    }
  },
  "Exclude": { //Replace with "Include" if you prefer to include Regions.
    "Regions": [
      "eu-west-1"
    ],
    "Buckets": [ //This attribute is not supported for AWS Organizations-level
configurations.
      "arn:aws:s3:::amzn-s3-demo-source-bucket "
    ]
  },
  "IsEnabled": true, //Whether the configuration is enabled
  "DataExport": { //Details about the metrics export
    "S3BucketDestination": {
      "OutputSchemaVersion": "V_1",
      "Format": "CSV", //You can add "Parquet" if you prefer.
      "AccountId": "111122223333",
      "Arn": "arn:aws:s3:::amzn-s3-demo-destination-bucket", // The destination
bucket for your metrics export must be in the same Region as your S3 Storage Lens
configuration.
      "Prefix": "prefix-for-your-export-destination",
      "Encryption": {
        "SSES3": {}
      }
    },
    "CloudWatchMetrics": {
      "IsEnabled": true //Mark this as false if you want to export only free metrics.
    }
```

```
  }
}
```

Utilisation du AWS SDK pour Java

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.ActivityMetrics;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.CloudWatchMetrics;
import com.amazonaws.services.s3control.model.Format;
import com.amazonaws.services.s3control.model.Include;
import com.amazonaws.services.s3control.model.OutputSchemaVersion;
import com.amazonaws.services.s3control.model.PrefixLevel;
import com.amazonaws.services.s3control.model.PrefixLevelStorageMetrics;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.S3BucketDestination;
import com.amazonaws.services.s3control.model.SSES3;
import com.amazonaws.services.s3control.model.SelectionCriteria;
import com.amazonaws.services.s3control.model.StorageLensAwsOrg;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensDataExport;
import com.amazonaws.services.s3control.model.StorageLensDataExportEncryption;
import com.amazonaws.services.s3control.model.StorageLensTag;

import java.util.Arrays;
import java.util.List;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateAndUpdateDashboard {

    public static void main(String[] args) {
        String configurationId = "ConfigurationId";
        String sourceAccountId = "Source Account ID";
        String exportAccountId = "Destination Account ID";
```

```
        String exportBucketArn = "arn:aws:s3:::amzn-s3-demo-destination-bucket"; //
 The destination bucket for your metrics export must be in the same Region as your S3
 Storage Lens configuration.
        String awsOrgARN = "arn:aws:organizations::123456789012:organization/o-
abcdefgh";
        Format exportFormat = Format.CSV;

        try {
            SelectionCriteria selectionCriteria = new SelectionCriteria()
                    .withDelimiter("/")
                    .withMaxDepth(5)
                    .withMinStorageBytesPercentage(10.0);
            PrefixLevelStorageMetrics prefixStorageMetrics = new
 PrefixLevelStorageMetrics()
                    .withIsEnabled(true)
                    .withSelectionCriteria(selectionCriteria);
            BucketLevel bucketLevel = new BucketLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withPrefixLevel(new
 PrefixLevel().withStorageMetrics(prefixStorageMetrics));
            AccountLevel accountLevel = new AccountLevel()
                    .withActivityMetrics(new ActivityMetrics().withIsEnabled(true))
                    .withAdvancedCostOptimizationMetrics(new
 AdvancedCostOptimizationMetrics().withIsEnabled(true))
                    .withAdvancedDataProtectionMetrics(new
 AdvancedDataProtectionMetrics().withIsEnabled(true))
                    .withDetailedStatusCodesMetrics(new
 DetailedStatusCodesMetrics().withIsEnabled(true))
                    .withBucketLevel(bucketLevel);

            Include include = new Include()
                    .withBuckets(Arrays.asList("arn:aws:s3:::amzn-s3-demo-bucket"))
                    .withRegions(Arrays.asList("us-west-2"));

            StorageLensDataExportEncryption exportEncryption = new
 StorageLensDataExportEncryption()
                    .withSSES3(new SSES3());
            S3BucketDestination s3BucketDestination = new S3BucketDestination()
```

```
                .withAccountId(exportAccountId)
                .withArn(exportBucketArn)
                .withEncryption(exportEncryption)
                .withFormat(exportFormat)
                .withOutputSchemaVersion(OutputSchemaVersion.V_1)
                .withPrefix("Prefix");
        CloudWatchMetrics cloudWatchMetrics = new CloudWatchMetrics()
                .withIsEnabled(true);
        StorageLensDataExport dataExport = new StorageLensDataExport()
                .withCloudWatchMetrics(cloudWatchMetrics)
                .withS3BucketDestination(s3BucketDestination);

        StorageLensAwsOrg awsOrg = new StorageLensAwsOrg()
                .withArn(awsOrgARN);

        StorageLensConfiguration configuration = new StorageLensConfiguration()
                .withId(configurationId)
                .withAccountLevel(accountLevel)
                .withInclude(include)
                .withDataExport(dataExport)
                .withAwsOrg(awsOrg)
                .withIsEnabled(true);

        List<StorageLensTag> tags = Arrays.asList(
                new StorageLensTag().withKey("key-1").withValue("value-1"),
                new StorageLensTag().withKey("key-2").withValue("value-2")
        );

        AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(US_WEST_2)
                .build();

        s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
                .withAccountId(sourceAccountId)
                .withConfigId(configurationId)
                .withStorageLensConfiguration(configuration)
                .withTags(tags)
        );
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 couldn't process
        // it and returned an error response.
        e.printStackTrace();
```

```
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Utilisation de l'API REST

Pour activer l'option de CloudWatch publication à l'aide de l'API REST Amazon S3, vous pouvez utiliser PutStorageLensConfiguration.

Étapes suivantes

Après avoir activé l'option de CloudWatch publication, vous pouvez accéder à vos métriques S3 Storage Lens dans CloudWatch. Vous pouvez également tirer parti CloudWatch des fonctionnalités pour surveiller et analyser les données de votre S3 Storage Lens dans CloudWatch. Pour plus d'informations, consultez les rubriques suivantes :

- Métriques et dimensions S3 Storage Lens
- Utilisation des métriques de S3 Storage Lens dans CloudWatch

Utilisation des métriques de S3 Storage Lens dans CloudWatch

Vous pouvez publier les métriques S3 Storage Lens sur Amazon CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatchtableaux de bord. Vous pouvez également utiliser des CloudWatch fonctionnalités, telles que les alarmes et les actions déclenchées, les mathématiques métriques et la détection des anomalies, pour surveiller et agir sur les métriques S3 Storage Lens. En outre, les opérations CloudWatch d'API permettent aux applications, y compris aux fournisseurs tiers, d'accéder à vos métriques S3 Storage Lens. Pour plus d'informations sur les CloudWatch fonctionnalités, consultez le guide de CloudWatch l'utilisateur Amazon.

Vous pouvez activer l'option de CloudWatch publication pour les configurations de tableau de bord nouvelles ou existantes à l'aide de la console Amazon S3 APIs AWS CLI, Amazon S3 REST et AWS SDKs. L'option de CloudWatch publication est disponible pour les tableaux de bord mis à niveau vers les métriques et recommandations avancées de S3 Storage Lens. Pour obtenir la tarification des métriques et recommandations avancées S3 Storage Lens, consultez Tarification Amazon S3. Aucun frais de publication de CloudWatch statistiques supplémentaires ne s'applique ; toutefois, d'autres

CloudWatch frais, tels que les tableaux de bord, les alarmes et les appels d'API, s'appliquent. Pour plus d'informations, consultez les CloudWatch tarifs Amazon.

Les métriques S3 Storage Lens sont publiées sur le compte propriétaire de la configuration S3 Storage Lens. CloudWatch Après avoir activé l'option de CloudWatch publication dans les métriques et recommandations avancées, vous pouvez accéder aux métriques au niveau de l'organisation, du compte et du bucket dans. CloudWatch Les métriques au niveau du préfixe ne sont pas disponibles dans. CloudWatch

> **Note**
>
> Les métriques S3 Storage Lens sont des statistiques quotidiennes publiées CloudWatch une fois par jour. Lorsque vous interrogez les métriques de S3 Storage Lens dans CloudWatch, la période de requête doit être de 1 jour (86 400 secondes). Une fois que vos métriques quotidiennes de S3 Storage Lens apparaissent dans votre tableau de bord S3 Storage Lens dans la console Amazon S3, l'affichage de ces mêmes métriques peut prendre quelques heures CloudWatch. Lorsque vous activez l'option de CloudWatch publication pour les métriques S3 Storage Lens pour la première fois, la publication de vos métriques peut prendre jusqu'à 24 heures CloudWatch.
> Actuellement, les métriques S3 Storage Lens ne peuvent pas être consommées par le biais de CloudWatch flux.

Pour plus d'informations sur l'utilisation des métriques S3 Storage Lens dans CloudWatch, consultez les rubriques suivantes.

Rubriques

- Utilisation de CloudWatch tableaux de bord
- Définition d'alarmes, déclenchement d'actions et utilisation de la détection d'anomalies
- Filtrage des métriques à l'aide de dimensions
- Calcul de nouvelles métriques avec des mathématiques appliquées aux métriques
- Utilisation d'expressions de recherche dans les graphiques

Utilisation de CloudWatch tableaux de bord

Vous pouvez utiliser CloudWatch des tableaux de bord pour surveiller les métriques de S3 Storage Lens ainsi que celles d'autres applications et créer une vue unifiée de l'état de santé de vos

opérations. Les tableaux de bord sont des pages d'accueil personnalisables dans la CloudWatch console que vous pouvez utiliser pour surveiller vos ressources dans une seule vue.

CloudWatch dispose d'un large contrôle des autorisations qui ne permet pas de limiter l'accès à un ensemble spécifique de mesures ou de dimensions. Les utilisateurs de votre compte ou de votre organisation qui y ont accès CloudWatch auront accès aux métriques pour toutes les configurations S3 Storage Lens pour lesquelles l'option d' CloudWatch assistance est activée. Vous ne pouvez pas gérer les autorisations pour des tableaux de bord spécifiques comme dans S3 Storage Lens. Pour plus d'informations sur CloudWatch les autorisations, consultez la section Gestion des autorisations d'accès à vos CloudWatch ressources dans le guide de CloudWatch l'utilisateur Amazon.

Pour plus d'informations sur l'utilisation CloudWatch des tableaux de bord et la configuration des autorisations, consultez les sections Utilisation des CloudWatch tableaux de bord Amazon et Partage de CloudWatch tableaux de bord dans le guide de l'utilisateur Amazon CloudWatch .

Définition d’alarmes, déclenchement d’actions et utilisation de la détection d’anomalies

Vous pouvez configurer des CloudWatch alarmes qui surveillent les métriques de S3 Storage Lens CloudWatch et prennent des mesures lorsqu'un seuil est dépassé. Par exemple, vous pouvez configurer une alarme qui envoie une notification Amazon SNS lorsque la métrique Incomplete Multipart Upload Bytes (Octets de chargements partitionnés non terminés) dépasse 1 Go pendant trois jours consécutifs.

Vous pouvez également activer la détection des anomalies pour analyser continuellement les métriques S3 Storage Lens, déterminer les références normales et les anomalies de surface. Vous pouvez créer une alarme de détection d’anomalie basée sur la valeur attendue d’une métrique. Par exemple, vous pouvez surveiller les anomalies pour la métrique Object Lock Enabled Bytes (Octets activés par le verrouillage d'objets) afin de détecter la suppression non autorisée des paramètres de verrouillage d'objets.

Pour plus d'informations et des exemples, consultez les sections Utilisation des CloudWatch alarmes Amazon et Création d'une alarme à partir d'une métrique sur un graphique dans le guide de CloudWatch l'utilisateur Amazon.

Filtrage des métriques à l’aide de dimensions

Vous pouvez utiliser les dimensions pour filtrer les métriques S3 Storage Lens dans la CloudWatch console. Par exemple, vous pouvez filtrer par `configuration_id`, `aws_account_number`, `aws_region`, `bucket_name` et plus encore.

S3 Storage Lens prend en charge plusieurs configurations de tableau de bord par compte. Cela signifie que différentes configurations peuvent inclure le même compartiment. Lorsque ces métriques sont publiées sur CloudWatch, le bucket contiendra des métriques dupliquées CloudWatch. Pour afficher les métriques uniquement pour une configuration spécifique de S3 Storage Lens dans CloudWatch, vous pouvez utiliser la `configuration_id` dimension. Lorsque vous filtrez par `configuration_id`, vous ne voyez que les métriques associées à la configuration que vous identifiez.

Pour plus d'informations sur le filtrage par ID de configuration, consultez la section Recherche des métriques disponibles dans le guide de CloudWatch l'utilisateur Amazon.

Calcul de nouvelles métriques avec des mathématiques appliquées aux métriques

Vous pouvez utiliser les mathématiques appliquées aux métriques pour interroger plusieurs métriques S3 Storage Lens et utiliser des expressions mathématiques pour créer des séries temporelles basées sur ces métriques. Par exemple, vous pouvez créer une nouvelle métrique pour les objets non chiffrés en soustrayant les objets chiffrés du nombre d'objets. Vous pouvez également créer une métrique pour obtenir la taille d'objet moyenne en divisant `StorageBytes` par `ObjectCount` ou le nombre d'octets consultés en un jour en divisant `BytesDownloaded` par `StorageBytes`.

Pour plus d'informations, consultez la section Utilisation des mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.

Utilisation d'expressions de recherche dans les graphiques

Avec les métriques S3 Storage Lens, vous pouvez créer une expression de recherche. Par exemple, vous pouvez créer une expression de recherche pour toutes les métriques nommées IncompleteMultipartUploadStorageByteset ajoutées `SUM` à l'expression. Avec cette expression de recherche, vous pouvez voir le nombre total d'octets de chargements partitionnés non terminés dans toutes les dimensions de votre stockage dans une seule métrique.

Cet exemple montre la syntaxe que vous utiliseriez pour créer une expression de recherche pour toutes les métriques nommées IncompleteMultipartUploadStorageBytes.

```
SUM(SEARCH('{AWS/S3/Storage-
Lens,aws_account_number,aws_region,configuration_id,metrics_version,record_type,storage_class}
 MetricName="IncompleteMultipartUploadStorageBytes"', 'Average',86400))
```

Pour plus d'informations sur cette syntaxe, consultez la section Syntaxe des expressions de CloudWatch recherche dans le guide de CloudWatch l'utilisateur Amazon. Pour créer un CloudWatch graphique avec une expression de recherche, consultez la section Création d'un CloudWatch graphique avec une expression de recherche dans le guide de CloudWatch l'utilisateur Amazon.

Cas d'utilisation des métriques Amazon S3 Storage Lens

Vous pouvez utiliser votre tableau de bord Amazon S3 Storage Lens pour visualiser les informations et les tendances, signaler les anomalies et recevoir des recommandations. Les métriques S3 Storage Lens sont organisées en catégories qui correspondent aux principaux cas d'utilisation. Vous pouvez utiliser ces métriques pour effectuer les opérations suivantes :

- Identifier les opportunités d'optimisation des coûts
- Appliquer les bonnes pratiques de protection des données
- Appliquer les bonnes pratiques de gestion des accès
- Améliorer les performances des charges de travail d'application

Par exemple, les métriques sur l'optimisation des coûts vous permettent d'identifier les opportunités pour réduire vos coûts de stockage Amazon S3. Vous pouvez identifier les compartiments contenant des chargements partitionnés datant de plus de 7 jours ou des compartiments qui accumulent d'anciennes versions.

De même, vous pouvez utiliser des métriques sur la protection des données pour identifier les compartiments qui ne respectent pas les bonnes pratiques de protection des données au sein de votre organisation. Par exemple, vous pouvez identifier les compartiments qui n'utilisent pas de AWS Key Management Service clés (SSE-KMS) pour le chiffrement par défaut ou pour lesquels le versionnage S3 n'est pas activé.

Grâce aux métriques de gestion des accès de S3 Storage Lens, vous pouvez identifier les paramètres de compartiment pour S3 Object Ownership afin de pouvoir migrer les autorisations de liste de contrôle d'accès (ACL) vers les politiques de compartiment et les désactiver. ACLs

Si vous avez activé S3 Storage Lens advanced metrics (Métriques avancées S3 Storage Lens), vous pouvez utiliser des métriques de codes de statut détaillés pour obtenir les nombres de demandes ayant réussi et échoué que vous pouvez utiliser pour résoudre les problèmes d'accès et de performances.

Grâce aux métriques avancées, vous pouvez également accéder à des métriques supplémentaires sur l'optimisation des coûts et la protection des données que vous pouvez utiliser pour identifier les

opportunités de réduire encore vos coûts globaux de stockage S3 et de mieux vous aligner sur les bonnes pratiques pour protéger vos données. Par exemple, les métriques avancées sur l'optimisation des coûts incluent les nombres de règles de cycle de vie que vous pouvez utiliser pour identifier les compartiments qui ne disposent pas de règles de cycle de vie pour faire expirer les chargements partitionnés non terminés datant de plus de 7 jours. Les métriques avancées sur la protection des données incluent les nombres de règles de réplication.

Pour plus d'informations sur les catégories de métriques, consultez Catégories de métriques. Pour obtenir la liste complète des métriques S3 Storage Lens, consultez Glossaire des métriques Amazon S3 Storage Lens.

Rubriques

- Utiliser Amazon S3 Storage Lens pour optimiser vos coûts de stockage
- Utilisation de S3 Storage Lens pour protéger vos données
- Utilisation de S3 Storage Lens pour auditer les paramètres de propriété d'objets
- Utilisation de métriques S3 Storage Lens pour améliorer les performances

Utiliser Amazon S3 Storage Lens pour optimiser vos coûts de stockage

Vous pouvez utiliser les métriques sur l'optimisation des coûts S3 Storage Lens pour réduire le coût global de votre stockage S3. Les métriques sur l'optimisation des coûts peuvent vous aider à confirmer que vous avez configuré Amazon S3 de manière rentable et conformément aux bonnes pratiques. Par exemple, vous pouvez identifier les opportunités d'optimisation des coûts suivantes :

- Compartiments contenant des chargements partitionnés non terminés datant de plus de 7 jours
- Compartiments qui accumulent de nombreuses versions anciennes
- Compartiments dépourvus de règles de cycle de vie pour abandonner les chargements partitionnés non terminés
- Compartiments dépourvus de règles de cycle de vie pour faire expirer des objets de version ancienne
- Compartiments dépourvus de règles de cycle de vie pour transférer des objets vers une autre classe de stockage

Vous pouvez ensuite utiliser ces données pour ajouter des règles de cycle de vie supplémentaires à vos compartiments.

Les exemples suivants montrent comment utiliser les métriques sur l'optimisation des coûts dans votre tableau de bord S3 Storage Lens pour optimiser vos coûts de stockage.

Rubriques

- Identifier vos compartiments S3 les plus importants
- Découverte des compartiments Amazon S3 froids
- Localiser les chargements partitionnés incomplets
- Réduire le nombre de versions anciennes conservées
- Identification des compartiments dépourvus de règles de cycle de vie et examen des nombres de règles de cycle de vie

Identifier vos compartiments S3 les plus importants

Des frais de stockage d'objets dans les compartiments S3 vous sont facturés. Le tarif qui vous est facturé dépend de la taille de vos objets, de leur durée de stockage et de leurs classes de stockage. Avec S3 Storage Lens, vous obtenez une vue centralisée de tous les compartiments figurant dans votre compte. Pour voir tous les compartiments de tous les comptes de votre organisation, vous pouvez configurer un tableau de bord S3 Storage Lens AWS Organizations au niveau 3. À partir de cette vue de tableau de bord, vous pouvez identifier vos compartiments les plus importants.

Étape 1 : identifier vos plus grands compartiments

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.

   Lorsque le tableau de bord s'ouvre, vous pouvez consulter la date la plus récente pour laquelle S3 Storage Lens a collecté des métriques. Votre tableau de bord se charge toujours à la date la plus récente pour laquelle des métriques sont disponibles.
4. Pour voir le classement de vos plus grands compartiments selon la métrique Stockage total pour une plage de dates sélectionnée, faites défiler l'écran jusqu'à la section Aperçu des N éléments principaux pour date.

Vous pouvez modifier l'ordre de tri pour afficher les plus petits compartiments. Vous pouvez également ajuster la sélection Metric (Métrique) pour classer vos compartiments en fonction d'une métrique disponible quelconque. La section Aperçu des N éléments principaux pour date indique également la variation en pourcentage par rapport à la journée ou à la semaine précédente et une ligne étincelante pour visualiser la tendance. Cette tendance est une tendance sur 14 jours pour les métriques gratuites et une tendance sur 30 jours pour les métriques et recommandations avancées.

> **Note**
>
> Grâce aux métriques et recommandations avancées S3 Storage Lens, les métriques sont disponibles pour les requêtes pendant 15 mois. Pour de plus amples informations, veuillez consulter Sélection des métriques.

5. Pour obtenir des informations plus détaillées sur vos compartiments, faites défiler la page vers le haut, puis choisissez l'onglet Bucket (Compartiment).

   Dans l'onglet Bucket (Compartiment), vous pouvez voir des détails tels que le taux de croissance récent, la taille moyenne d'objet, les préfixes les plus importants et le nombre d'objets.

Étape 2 : accéder à vos compartiments et mener des investigations

Après avoir identifié vos compartiments S3 les plus importants, vous pouvez accéder à chacun d'eux dans la console S3 pour consulter les objets y figurant, comprendre sa charge de travail associée et identifier ses propriétaires internes. Vous pouvez contacter les propriétaires des compartiments pour déterminer si cette croissance est attendue ou si elle a besoin d'une surveillance et d'un contrôle plus poussés.

Découverte des compartiments Amazon S3 froids

Si vous avez activé S3 Storage Lens advanced metrics (Métriques avancées S3 Storage Lens), vous pouvez utiliser des métriques d'activité pour comprendre à quel point vos compartiments S3 sont froids. Un compartiment « froid » est un compartiment dont on accède plus (ou très rarement) au stockage. Ce manque d'activité indique généralement que l'on n'accède pas fréquemment aux objets du compartiment.

Les métriques d'activité, telles que Get Requests (Demandes Get) et Download Bytes (Octets de chargement) indiquent la fréquence d'accès quotidien à vos compartiments. Pour comprendre la

cohérence du modèle d'accès et pour repérer les compartiments auxquels on n'accède plus du tout, vous pouvez modifier ces données sur plusieurs mois. La métrique Retrieval Rate (Taux d'extraction), qui est calculée en tant qu'octets de téléchargement/Stockage total, indique la proportion de stockage dans un compartiment auquel on accède quotidiennement.

> **Note**
>
> Les octets de téléchargement sont dupliqués dans les cas où le même objet est téléchargé plusieurs fois au cours de la journée.

Prérequis

Pour voir les métriques d'activité dans votre tableau de bord S3 Storage Lens, vous devez activer Advanced metrics and recommendations (Métriques et recommandations avancées) S3 Storage Lens, puis sélectionner Activity metrics (Métriques d'activité). Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

Étape 1 : identifier les compartiments actifs

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.
4. Choisissez l'onglet Bucket (Compartiment) et faites défiler l'écran jusqu'à la section Bubble analysis by buckets for date (Analyse à bulles par compartiments pour date).

   Dans la section Bubble analysis by buckets for date (Analyse à bulles par compartiments pour date), vous pouvez tracer vos compartiments sur plusieurs dimensions à l'aide de trois métriques quelconques pour représenter les valeurs X-axis (Axe des X), Y-axis (Axe des Y) et Size (Taille) de la bulle.
5. Pour rechercher les compartiments devenus froids, pour X-axis (Axe des X), Y-axis (Axe des Y) et Size (Taille), choisissez les métriques Total storage (Stockage total), % retrieval rate (Taux d'extraction en %) et Average object size (Taille moyenne des objets).
6. Dans la section Bubble analysis by buckets for date (Analyse à bulles par compartiments pour date), localisez les compartiments dont le taux d'extraction est égal à zéro (ou proche de zéro)

et ayant une taille de stockage relative plus grande, et choisissez la bulle qui représente le compartiment.

Une case apparaît avec des choix pour afficher des informations plus détaillées. Effectuez l'une des actions suivantes :

a. Pour mettre à jour l'onglet Bucket (Compartiment) afin d'afficher les métriques uniquement pour le compartiment sélectionné, choisissez Drill down (Approfondir), puis choisissez Apply (Appliquer).
b. Pour agréger vos données au niveau du compartiment par compte Région AWS, classe de stockage ou compartiment, choisissez Analyser par, puis choisissez Dimension. Par exemple, pour agréger par classe de stockage, choisissez Storage class (Classe de stockage) pour Dimension.

Pour trouver des compartiments qui sont devenus froids, effectuez une analyse à bulles à l'aide des métriques Total storage (Stockage total), % Retrieval Rate (% de taux d'extraction) et Average object size (Taille moyenne des objets). Recherchez les compartiments dont le taux de récupération est égal à zéro (ou proche de zéro) et ayant une taille de stockage relative plus grande.

L'onglet Bucket (Compartiment) de votre tableau de bord est mis à jour pour afficher les données relatives à l'agrégation ou au filtre que vous avez sélectionné(e). Si vous avez agrégé par classe de stockage ou par une autre dimension, ce nouvel onglet s'ouvre dans votre tableau de bord (par exemple, l'onglet Storage class (Classe de stockage)).

Étape 2 : mener des investigations sur les compartiments froids

À ce stade, vous pouvez identifier les propriétaires des compartiments froids dans votre compte ou votre organisation et déterminer si ce stockage est toujours nécessaire. Vous pouvez ensuite optimiser les coûts avec des configurations d'expiration de cycle de vie pour ces compartiments ou en archivant des données dans l'une des classes de stockage Amazon S3 Glacier.

Pour éviter le problème des compartiments froids à l'avenir, vous pouvez effectuer une transition automatique de vos données à l'aide de configurations de cycle de vie S3 pour vos compartiments, ou vous pouvez activer l'archivage automatique avec S3 Intelligent-Tiering.

Vous pouvez également utiliser l'étape 1 pour identifier les compartiments chauds. Ensuite, vous pouvez vous assurer que ces compartiments utilisent la classe de stockage S3 appropriée afin de répondre à leurs demandes de la manière la plus efficace en termes de performances et de coûts.

Localiser les chargements partitionnés incomplets

Vous pouvez utiliser les chargements partitionnés pour charger des objets de très grande taille (jusqu'à 5 To) en tant qu'ensemble de parties pour améliorer le débit et accélérer la récupération suite à des problèmes réseau. Dans les cas où le processus de chargement partitionné ne se termine pas, les parties incomplètes restent dans le compartiment (dans un état inutilisable). Ces parties incomplètes entraînent des coûts de stockage jusqu'à la fin du processus de chargement ou jusqu'à leur suppression. Pour de plus amples informations, veuillez consulter Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.

Avec S3 Storage Lens, vous pouvez identifier le nombre d'octets des chargements partitionnés non terminés dans votre compte ou dans l'ensemble de votre organisation, y compris les chargements partitionnés non terminés datant de plus de 7 jours. Pour obtenir la liste complète des métriques des chargements partitionnés non terminés, consultez Glossaire des métriques Amazon S3 Storage Lens.

À titre de bonne pratique, nous vous recommandons de configurer des règles de cycle de vie pour faire expirer les chargements partitionnés non terminés datant de plus d'un certain nombre de jours. Lorsque vous créez votre règle de cycle de vie pour faire expirer les chargements partitionnés non terminés, nous recommandons un délai de 7 jours comme point de départ.

Étape 1 : passer en revue les tendances générales relatives aux chargements partitionnés non terminés

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.
4. Dans la section Snapshot for date (Instantané pour date), sous Metrics categories (Catégories de métriques), choisissez Cost optimization (Optimisation des coûts).

   La section Instantané pour date est mise à jour pour afficher les métriques Optimisation des coûts, qui incluent Octets de chargements partitionnés non terminés datant de plus de 7 jours.

Dans n'importe quel graphique de votre tableau de bord S3 Storage Lens, vous pouvez consulter les métriques des chargements partitionnés non terminés. Vous pouvez utiliser ces métriques pour évaluer plus en détail l'impact des octets des chargements partitionnés non terminés sur votre stockage, y compris leur contribution aux tendances générales de croissance. Vous pouvez également accéder à des niveaux d'agrégation plus profonds en utilisant les onglets Account (Compte), Région AWS, Bucket (Compartiment) ou Storage class (Classe de stockage) pour une analyse approfondie de vos données. Pour obtenir un exemple, consultez Découverte des compartiments Amazon S3 froids.

Étape 2 : identifier les compartiments contenant le plus grand nombre d'octets de chargements partitionnés non terminés mais ne disposant pas de règles de cycle de vie permettant d'abandonner les chargements partitionnés non terminés

Prérequis

Pour consulter la métrique Abort incomplete multipart upload lifecycle rule count (Nombre de règles de cycle de vie d'abandon de chargements partitionnés non terminés) dans votre tableau de bord S3 Storage Lens, vous devez activer Advanced metrics and recommendations (Métriques et recommandations avancées) S3 Storage Lens, puis sélectionner Advanced cost optimization metrics (Métriques avancées d'optimisation des coûts). Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.
4. Pour identifier les compartiments spécifiques qui accumulent des chargements partitionnés non terminés datant de plus de 7 jours, accédez à la section Aperçu des N éléments principaux pour date.

   Par défaut, la section Aperçu des N éléments principaux pour date affiche les métriques des 3 principaux compartiments. Vous pouvez augmenter ou diminuer le nombre de compartiments dans le champ Top N (N éléments principaux). La section Top N overview for date (Aperçu des N éléments principaux pour date) indique également la variation en pourcentage par rapport

à la journée ou à la semaine précédente et une ligne étincelante pour visualiser la tendance. (Cette tendance est une tendance sur 14 jours pour les métriques gratuites et une tendance sur 30 jours pour les métriques et recommandations avancées.)

> **Note**
>
> Grâce aux métriques et recommandations avancées S3 Storage Lens, les métriques sont disponibles pour les requêtes pendant 15 mois. Pour de plus amples informations, veuillez consulter Sélection des métriques.

5. Pour Métrique, choisissez Octets de chargements partitionnés non terminés datant de plus de 7 jours dans la catégorie Optimisation des coûts.

   Sous Top number buckets (nombre compartiments principaux), vous pouvez voir les compartiments contenant le plus d'octets de chargements partitionnés non terminés datant de plus de 7 jours.

6. Pour afficher des métriques plus détaillées au niveau des compartiments pour les chargements partitionnés non terminés, faites défiler l'affichage jusqu'en haut de la page, puis choisissez l'onglet Bucket (Compartiment).

7. Faites défiler jusqu'à la section Buckets (Compartiments). Pour Metrics categories (Catégories de métriques), sélectionnez Cost optimization (Optimisation des coûts). Effacez ensuite Summary (Résumé).

   La liste Buckets (Compartiments) est mise à jour pour afficher toutes les métriques Cost optimization (Optimisation des coûts) disponibles pour les compartiments affichés.

8. Pour filtrer la liste Buckets (Compartiments) afin d'afficher uniquement les métriques sur l'optimisation des coûts spécifiques, choisissez l'icône des préférences ( ).

9. Désactivez les boutons bascules pour toutes les métriques sur l'optimisation des coûts jusqu'à ce que seules les métriques Octets de chargements partitionnés non terminés datant de plus de 7 jours et Nombre de règles de cycle de vie d'abandon de chargements partitionnés non terminés restent sélectionnées.

10. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.

11. Choisissez Confirmer.

La liste Buckets (Compartiments) est mise à jour pour afficher les métriques au niveau des compartiments pour les chargements partitionnés non terminés et les nombres de règles de cycle de vie. Vous pouvez utiliser ces données pour identifier les compartiments contenant le plus grand nombre d'octets de chargements partitionnés non terminés datant de plus de 7 jours et ne présentant pas de règles de cycle de vie permettant d'abandonner les chargements partitionnés non terminés. Ensuite, vous pouvez accéder à ces compartiments dans la console S3 et ajouter des règles de cycle de vie pour supprimer les chargements partitionnés non terminés abandonnés.

Étape 3 : ajouter une règle de cycle de vie pour supprimer les chargements partitionnés non terminés après 7 jours

Pour gérer automatiquement les chargements partitionnés non terminés, vous pouvez utiliser la console S3 pour créer une configuration de cycle de vie afin de faire expirer les octets de chargements partitionnés non terminés d'un compartiment après un nombre de jours spécifié. Pour de plus amples informations, veuillez consulter Configuration d'une configuration de cycle de vie de compartiment pour supprimer les chargements partitionnés incomplets.

Réduire le nombre de versions anciennes conservées

Lorsque cette option est activée, la fonction de gestion des versions S3 conserve plusieurs copies distinctes du même objet que vous pouvez utiliser pour récupérer rapidement les données si un objet est supprimé ou écrasé accidentellement. Si vous avez activé la gestion des versions S3 sans configurer de règles de cycle de vie pour faire passer ou expirer des versions anciennes, un grand nombre de versions anciennes peuvent s'accumuler, ce qui peut avoir des répercussions sur les coûts de stockage. Pour de plus amples informations, veuillez consulter Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Étape 1 : identifier les compartiments contenant le plus grand nombre de versions d'objet anciennes

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.

4. Dans la section Snapshot for date (Instantané pour date), sous Metric categories (Catégories de métriques), choisissez Cost optimization (Optimisation des coûts).

   La section Instantané pour date est mise à jour pour afficher les métriques Optimisation des coûts, qui incluent la métrique % d'octets de version ancienne. La métrique % d'octets de version ancienne représente la proportion du nombre total d'octets de stockage qui est attribuée à des versions anciennes, dans la portée du tableau de bord et pour la date sélectionnée.

   > **Note**
   >
   > Si votre métrique % d'octets de version ancienne est supérieure à 10 % de votre stockage au niveau du compte, cela peut indiquer que vous stockez trop de versions d'objet.

5. Pour identifier des compartiments spécifiques qui accumulent un grand nombre de versions anciennes :

   a. Faites défiler l'écran vers le bas jusqu'à la section Aperçu des N éléments principaux pour date. Pour Top N (N éléments principaux), entrez le nombre de compartiments pour lesquels vous souhaitez voir des données.

   b. Pour Métrique, choisissez % d'octets de version ancienne.

      Sous nombre compartiments principaux, vous pouvez voir les compartiments (pour le nombre que vous avez spécifié) avec la métrique % d'octets de version ancienne la plus élevée. La section Top N overview for date (Aperçu des N éléments principaux pour date) indique également la variation en pourcentage par rapport à la journée ou à la semaine précédente et une ligne étincelante pour visualiser la tendance. Cette tendance est une tendance sur 14 jours pour les métriques gratuites et une tendance sur 30 jours pour les métriques et recommandations avancées.

      > **Note**
      >
      > Grâce aux métriques et recommandations avancées S3 Storage Lens, les métriques sont disponibles pour les requêtes pendant 15 mois. Pour de plus amples informations, veuillez consulter Sélection des métriques.

c. Pour afficher des métriques plus détaillées au niveau des compartiments pour les versions d'objet anciennes, faites défiler l'affichage jusqu'en haut de la page, puis choisissez l'onglet Bucket (Compartiment).

   Dans un graphique ou une visualisation quelconque de votre tableau de bord S3 Storage Lens, vous pouvez accéder à des niveaux d'agrégation plus approfondis à l'aide des onglets Account (Compte), Région AWS, Storage class (Classe de stockage) ou Bucket (Compartiment). Pour obtenir un exemple, consultez Découverte des compartiments Amazon S3 froids.

d. Dans la section Buckets (Compartiments), pour Metric categories (Catégories de métriques), sélectionnez Cost optimization (Optimisation des coûts). Effacez ensuite Summary (Résumé).

   Vous pouvez désormais voir la métrique % d'octets de version ancienne, ainsi que d'autres métriques relatives aux versions anciennes.

Étape 2 : identifier les compartiments auxquels il manque des règles de cycle de vie de transition et d'expiration pour la gestion des versions anciennes

Prérequis

Pour consulter les métriques Nombre de règles de cycle de vie des transitions de version ancienne et Nombre de règles de cycle de vie d'expiration de version ancienne dans votre tableau de bord S3 Storage Lens, vous devez activer Métriques et recommandations avancées S3 Storage Lens, puis sélectionner Métriques avancées d'optimisation des coûts. Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.
4. Dans votre tableau de bord Storage Lens, choisissez l'onglet Bucket (Compartiment).
5. Faites défiler jusqu'à la section Buckets (Compartiments). Pour Metrics categories (Catégories de métriques), sélectionnez Cost optimization (Optimisation des coûts). Effacez ensuite Summary (Résumé).

La liste Buckets (Compartiments) est mise à jour pour afficher toutes les métriques Cost optimization (Optimisation des coûts) disponibles pour les compartiments affichés.

6. Pour filtrer la liste Buckets (Compartiments) afin d'afficher uniquement les métriques sur l'optimisation des coûts spécifiques, choisissez l'icône des préférences ().
7. Désactivez les boutons bascules pour toutes les métriques sur l'optimisation des coûts jusqu'à ce que seules les métriques suivantes restent sélectionnées :
   - % d'octets de version ancienne
   - Nombre de règles de cycle de vie des transitions de version ancienne
   - Nombre de règles de cycle de vie d'expiration de version ancienne
8. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.
9. Choisissez Confirmer.

   La liste Compartiments est mise à jour pour afficher les métriques relatives aux octets de version ancienne et aux nombres de règles de cycle de vie de version ancienne. Vous pouvez utiliser ces données pour identifier les compartiments qui contiennent un pourcentage élevé d'octets de version ancienne mais auxquels il manque des règles de cycle de vie de transition et d'expiration. Vous pouvez ensuite accéder à ces compartiments dans la console S3 et leur ajouter des règles de cycle de vie.

Étape 3 : ajouter des règles de cycle de vie pour transférer ou faire expirer des versions d'objet anciennes

Une fois que vous avez déterminé quels compartiments doivent être examinés davantage, vous pouvez accéder aux compartiments dans la console S3 et ajouter une politique de cycle de vie pour faire expirer les versions anciennes après un nombre de jours spécifié. Pour réduire les coûts tout en conservant les versions non actuelles, vous pouvez également configurer une règle de cycle de vie pour transférer les versions non actuelles vers l'une des classes de Amazon S3 Glacier stockage. Pour de plus amples informations, veuillez consulter Spécification d'une règle de cycle de vie pour un compartiment avec gestion des versions.

Identification des compartiments dépourvus de règles de cycle de vie et examen des nombres de règles de cycle de vie

S3 Storage Lens fournit des métriques relatives aux nombres de règles de cycle de vie S3 que vous pouvez utiliser pour identifier les compartiments auxquels il manque des règles de cycle de vie. Pour rechercher les compartiments dépourvus de règles de cycle de vie, vous pouvez utiliser la métrique Total buckets without lifecycle rules (Nombre total de compartiments sans règles de cycle de vie). Un compartiment sans configuration de cycle de vie S3 peut contenir un espace de stockage dont vous n'avez plus besoin ou que vous pouvez migrer vers une classe de stockage moins coûteuse. Vous pouvez également utiliser des métriques relatives aux nombres de règles de cycle de vie pour identifier les compartiments auxquels il manque des types spécifiques de règles de cycle de vie, tels que des règles d'expiration ou de transition.

Prérequis

Pour consulter les métriques relatives aux nombres de règles de cycle de vie et la métrique Total buckets without lifecycle rules (Nombre total de compartiments sans règles de cycle de vie) dans votre tableau de bord S3 Storage Lens, vous devez activer Advanced metrics and recommendations (Métriques et recommandations avancées) S3 Storage Lens, puis sélectionner Advanced cost optimization metrics (Métriques avancées sur l'optimisation des coûts). Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

Étape 1 : identifier les compartiments sans règles de cycle de vie

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.
4. Pour identifier des compartiments spécifiques sans règles de cycle de vie, faites défiler l'affichage vers le bas jusqu'à la section Aperçu des N éléments principaux pour date.

   Par défaut, la section Top N overview for date (Aperçu des N éléments principaux pour date) affiche les métriques des 3 principaux compartiments. Dans le champ Top N (N éléments principaux), vous pouvez augmenter le nombre de compartiments. La section Top N overview for date (Aperçu des N éléments principaux pour date) indique également la variation en pourcentage par rapport à la journée ou à la semaine précédente et une ligne étincelante pour

visualiser la tendance. Cette tendance est une tendance sur 14 jours pour les métriques gratuites et une tendance sur 30 jours pour les métriques et recommandations avancées.

> **Note**
>
> Grâce aux métriques et recommandations avancées S3 Storage Lens, les métriques sont disponibles pour les requêtes pendant 15 mois. Pour de plus amples informations, veuillez consulter Sélection des métriques.

5. Pour Metric (Métrique), choisissez Total buckets without lifecycle rules (Nombre total de compartiments sans règles de cycle de vie) dans la catégorie Cost optimization (Optimisation des coûts).
6. Consultez les données suivantes pour Total buckets without lifecycle rules (Nombre total de compartiments sans règles de cycle de vie) :

   - Top number accounts (nombre comptes principaux) – Découvrez les comptes qui contiennent le plus de compartiments sans règles de cycle de vie.
   - nombre régions principales : consultez la répartition des compartiments sans règles de cycle de vie par région.
   - Top number buckets (nombre compartiments principaux) – Découvrez quels compartiments sont dépourvus de règles de cycle de vie.

   Dans un graphique ou une visualisation quelconque de votre tableau de bord S3 Storage Lens, vous pouvez accéder à des niveaux d'agrégation plus approfondis à l'aide des onglets Account (Compte), Région AWS, Storage class (Classe de stockage) ou Bucket (Compartiment). Pour obtenir un exemple, consultez Découverte des compartiments Amazon S3 froids.

   Après avoir identifié les compartiments dépourvus de règles de cycle de vie, vous pouvez également passer en revue les nombres de règles de cycle de vie spécifiques pour vos compartiments.

Étape 2 : passer en revue les nombres de règles de cycle de vie pour vos compartiments

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), sélectionnez le tableau de bord que vous souhaitez afficher.
4. Dans votre tableau de bord S3 Storage Lens, choisissez l'onglet Bucket (Compartiment).
5. Faites défiler jusqu'à la section Buckets (Compartiments). Sous Metrics categories (Catégories de métriques), sélectionnez Cost optimization (Optimisation des coûts). Effacez ensuite Summary (Résumé).

   La liste Buckets (Compartiments) est mise à jour pour afficher toutes les métriques Cost optimization (Optimisation des coûts) disponibles pour les compartiments affichés.
6. Pour filtrer la liste Buckets (Compartiments) afin d'afficher uniquement les métriques sur l'optimisation des coûts spécifiques, choisissez l'icône des préférences ().
7. Désactivez les boutons bascules pour toutes les métriques sur l'optimisation des coûts jusqu'à ce que seules les métriques suivantes restent sélectionnées :

   - Nombre de règles de cycle de vie de transition
   - Nombre de règles de cycle de vie d'expiration
   - Noncurrent version transition lifecycle rule count (Nombre de règles de cycle de vie des transitions de version ancienne)
   - Noncurrent version expiration lifecycle rule count (Nombre de règles de cycle de vie d'expiration de version ancienne)
   - Abort incomplete multipart upload lifecycle rule count (Nombre de règles de cycle de vie d'abandon de chargements partitionnés non terminés)
   - Nombre total de règles de cycle de vie
8. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.
9. Choisissez Confirmer.

   La liste Buckets (Compartiments) est mise à jour pour afficher les métriques relatives aux nombres de règles de cycle de vie pour vos compartiments. Vous pouvez utiliser ces données pour identifier les compartiments sans règles de cycle de vie ou les compartiments auxquels il manque certains types de règles de cycle de vie, par exemple des règles d'expiration ou de

transition. Vous pouvez ensuite accéder à ces compartiments dans la console S3 et leur ajouter des règles de cycle de vie.

Étape 3 : ajouter des règles de cycle de vie

Après avoir identifié les compartiments sans règles de cycle de vie, vous pouvez ajouter des règles de cycle de vie. Pour plus d'informations, consultez Définition d'une configuration du cycle de vie S3 sur un compartiment et Exemples de configurations du cycle de vie S3.

Utilisation de S3 Storage Lens pour protéger vos données

Vous pouvez utiliser les métriques sur la protection des données Amazon S3 Storage Lens pour identifier les compartiments dans lesquels les bonnes pratiques de protection des données n'ont pas été appliquées. Vous pouvez utiliser ces métriques pour agir et appliquer des paramètres standard conformes aux bonnes pratiques pour protéger vos données dans les compartiments de votre compte ou de votre organisation. Par exemple, vous pouvez utiliser des mesures de protection des données pour identifier les compartiments qui n'utilisent pas de clés AWS Key Management Service (AWS KMS) (SSE-KMS) pour le chiffrement par défaut ou les demandes qui utilisent AWS Signature Version 2 (SIGv2).

Les cas d'utilisation suivants fournissent des stratégies d'utilisation de votre tableau de bord S3 Storage Lens pour identifier les anomalies et appliquer les bonnes pratiques de protection des données sur vos compartiments S3.

Rubriques

- Identifiez les compartiments qui n'utilisent pas le chiffrement côté serveur AWS KMS pour le chiffrement par défaut (SSE-KMS)
- Identification des compartiments pour lesquels la gestion des versions S3 est activée
- Identification des demandes qui utilisent AWS Signature Version 2 (SigV2)
- Décompte du nombre total de règles de réplication pour chaque compartiment
- Identification du pourcentage d'octets de verrouillage d'objets

Identifiez les compartiments qui n'utilisent pas le chiffrement côté serveur AWS KMS pour le chiffrement par défaut (SSE-KMS)

Avec le chiffrement par défaut d'Amazon S3, vous pouvez définir le comportement de chiffrement par défaut pour un compartiment S3. Pour de plus amples informations, veuillez consulter the section called "Définition du chiffrement du compartiment par défaut".

Vous pouvez utiliser les métriques du nombre de compartiments activés par SSE-KMS et du % de compartiments activés par SSE-KMS pour identifier les compartiments qui utilisent le chiffrement côté serveur avec des clés (SSE-KMS) comme chiffrement par AWS KMS défaut. S3 Storage Lens fournit également des métriques pour les octets non chiffrés, les objets non chiffrés, les octets chiffrés et les objets chiffrés. Pour obtenir une liste complète des métriques, consultez Glossaire des métriques Amazon S3 Storage Lens.

Vous pouvez analyser les métriques de chiffrement SSE-KMS dans le contexte des métriques de chiffrement générales afin d'identifier les compartiments qui n'utilisent pas SSE-KMS. Pour utiliser SSE-KMS pour tous les compartiments de votre compte ou de votre organisation, vous pouvez ensuite mettre à jour les paramètres de chiffrement par défaut de ces compartiments afin d'utiliser SSE-KMS. Outre SSE-KMS, vous pouvez utiliser le chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) ou des clés fournies par le client (SSE-C). Pour de plus amples informations, veuillez consulter Protection des données à l'aide du chiffrement.

Étape 1 : identifier les compartiments qui utilisent SSE-KMS pour le chiffrement par défaut

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans la section Tendances et distributions, choisissez % de compartiments avec SSE-KMS activé comme métrique principale et % d'octets chiffrés comme métrique secondaire.

   Le graphique Trend for date (Tendance pour date) est mis à jour pour afficher les tendances relatives à SSE-KMS et aux octets chiffrés.
5. Pour afficher des informations plus détaillées au niveau du compartiment pour SSE-KMS :

   a. Choisissez un point sur le graphique. Une case apparaît avec des choix pour afficher des informations plus détaillées.

b. Choisissez la dimension Buckets (Compartiments). Choisissez ensuite Appliquer.

6. Dans le graphique Distribution by buckets for date (Distribution par compartiments pour date), choisissez la métrique SSE-KMS enabled bucket count (Nombre de compartiments avec SSE-KMS activé).
7. Vous pouvez désormais voir pour quels compartiments SSE-KMS est activé et pour quels compartiments il ne l'est pas.

Étape 2 : mettre à jour les paramètres de chiffrement par défaut des compartiments

Maintenant que vous avez déterminé quels compartiments utilisent SSE-KMS dans le contexte de votre métrique % d'octets chiffrés, vous pouvez identifier les compartiments qui n'utilisent pas SSE-KMS. Vous pouvez ensuite éventuellement accéder à ces compartiments dans la console S3 et mettre à jour leurs paramètres de chiffrement par défaut pour utiliser SSE-KMS ou SSE-S3. Pour de plus amples informations, veuillez consulter Configuration du chiffrement par défaut.

Identification des compartiments pour lesquels la gestion des versions S3 est activée

Lorsque cette option est activée, la fonction de gestion des versions S3 conserve plusieurs versions du même objet qui peuvent être utilisées pour récupérer rapidement des données si un objet est supprimé ou écrasé accidentellement. Vous pouvez utiliser la métrique Versioning-enabled bucket count (Nombre de compartiments activés pour la gestion des versions) pour voir quels compartiments utilisent la gestion des versions S3. Ensuite, vous pouvez agir dans la console S3 pour activer la gestion des versions S3 pour d'autres compartiments.

Étape 1 : identifier les compartiments pour lesquels la gestion des versions S3 est activée

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation, choisissez Storage Lens, Tableaux de bord.
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans la section Trends and distributions (Tendances et distributions), choisissez Versioning-enabled bucket count (Nombre de compartiments activés pour la gestion des versions) comme métrique principale et Buckets (Compartiments) comme métrique secondaire.

   Le graphique Trend for date (Tendance pour date) est mis à jour pour afficher les tendances des compartiments pour lesquels la gestion des versions S3 est activée. Juste en dessous de la

courbe des tendances, vous pouvez voir les sous-sections Distribution des classes de stockage et Distribution par région.

5. Pour obtenir des informations plus détaillées sur l'un des compartiments que vous voyez dans le graphique Trend for date (Tendance pour date) afin de pouvoir effectuer une analyse approfondie, procédez comme suit :

   a. Choisissez un point sur le graphique. Une case apparaît avec des choix pour afficher des informations plus détaillées.

   b. Choisissez une dimension à appliquer à vos données pour une analyse plus approfondie : Account (Compte), Région AWS, Storage class (Classe de stockage) ou Bucket (Compartiment). Choisissez ensuite Appliquer.

6. Dans la section Bubble analysis by buckets for date (Analyse à bulles par compartiments pour date), choisissez les métriques Versioning-enabled bucket count (Nombre de compartiments activés pour la gestion des versions), Buckets (Compartiments) et Active buckets (Compartiments actifs).

   La section Bubble analysis by buckets for date (Analyse à bulles par compartiments pour date) est mise à jour pour afficher les données relatives aux métriques que vous avez sélectionnées. Vous pouvez utiliser ces données pour voir pour quels compartiments la gestion des versions S3 est activée dans le contexte de votre nombre total de compartiments. Dans la section Bubble analysis by buckets for date (Analyse à bulles par compartiments pour date), vous pouvez tracer vos compartiments sur plusieurs dimensions à l'aide de trois métriques quelconques pour représenter les valeurs X-axis (Axe des X), Y-axis (Axe des Y) et Size (Taille) de la bulle.

Étape 2 : activer la gestion des versions S3

Après avoir identifié les compartiments pour lesquels la gestion des versions S3 est activée, vous pouvez identifier les compartiments pour lesquels la gestion des versions S3 n'a jamais été activée ou a été suspendue. Ensuite, vous pouvez éventuellement activer la gestion des versions pour ces compartiments dans la console S3. Pour de plus amples informations, veuillez consulter Activation de la gestion des versions sur les compartiments.

Identification des demandes qui utilisent AWS Signature Version 2 (SigV2)

Vous pouvez utiliser la métrique Toutes les demandes de signature non prises en charge pour identifier les demandes utilisant la version 2 de AWS signature (SIGv2). Ces données peuvent vous aider à identifier les applications spécifiques qui utilisent SigV2. Vous pouvez ensuite migrer ces applications vers AWS Signature Version 4 (SigV4).

SigV4 est la méthode de signature recommandée pour toutes les nouvelles applications S3. Le SigV4 offre une sécurité améliorée et est pris en charge dans tous les Régions AWS domaines. Pour plus d'informations, consultez Amazon S3 update - SigV2 deprecation period extended & modified (Mise à jour Amazon S3 – Période d'obsolescence SigV2 étendue et modifiée).

Prérequis

Pour voir la métrique Toutes les demandes de signature non prises en charge dans votre tableau de bord S3 Storage Lens, vous devez activer Métriques et recommandations avancées de S3 Storage Lens, puis sélectionner Métriques avancées sur la protection des données. Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

Étape 1 : Examiner les tendances de signature SigV2 par région Compte AWS, par région et par compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Pour identifier des compartiments, des comptes et des régions spécifiques dont les demandes utilisent SigV2 :

    a. Sous Aperçu des N éléments principaux pour date, dans N éléments principaux, entrez le nombre de compartiments pour lesquels vous souhaitez voir des données.

    b. Pour Métrique, choisissez Toutes les demandes de signature non prises en charge dans la catégorie Protection des données.

    La liste Top N des mises à jour des dates afin d'afficher les données relatives aux demandes SIGv2 par compte et par compartiment. Région AWS La section Aperçu des N éléments principaux pour date indique également la variation en pourcentage par rapport à la journée ou à la semaine précédente et une ligne étincelante pour visualiser la tendance. Cette tendance est une tendance sur 14 jours pour les métriques gratuites et une tendance sur 30 jours pour les métriques et recommandations avancées.

> **Note**
>
> Grâce aux métriques et recommandations avancées S3 Storage Lens, les métriques sont disponibles pour les requêtes pendant 15 mois. Pour de plus amples informations, veuillez consulter Sélection des métriques.

Étape 2 : identifier les compartiments auxquels les applications accèdent via des demandes SigV2

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans votre tableau de bord Storage Lens, choisissez l'onglet Bucket (Compartiment).
5. Faites défiler jusqu'à la section Buckets (Compartiments). Sous Metrics categories (Catégories de métriques), choisissez Data protection (Protection des données). Effacez ensuite Summary (Résumé).

   La liste Buckets (Compartiments) est mise à jour pour afficher toutes les métriques Data protection (Protection des données) disponibles pour les compartiments affichés.
6. Pour filtrer la liste Buckets (Compartiments) afin d'afficher uniquement des métriques spécifiques sur la protection des données, choisissez l'icône des préférences ().
7. Désactivez les boutons bascules pour toutes les métriques sur la protection des données jusqu'à ce que seules les métriques suivantes restent sélectionnées :

   - Toutes les demandes de signature non prises en charge
   - % de toutes les demandes de signature non prises en charge
8. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.
9. Choisissez Confirmer.

La liste Buckets (Compartiments) est mise à jour pour afficher les métriques au niveau des compartiments pour les demandes SigV2. Vous pouvez utiliser ces données pour identifier des compartiments spécifiques qui font l'objet de demandes SigV2. Vous pouvez ensuite utiliser ces informations pour migrer vos applications vers SigV4. Pour plus d'informations, consultez Authentification des demandes (AWS Signature version 4) dans le manuel Amazon Simple Storage Service API Reference.

Décompte du nombre total de règles de réplication pour chaque compartiment

La réplication S3 permet la copie automatique et asynchrone d'objets entre les compartiments Amazon S3. Les compartiments configurés pour la réplication d'objet peuvent appartenir au même Compte AWS ou à des comptes distincts. Pour de plus amples informations, veuillez consulter Réplication d'objets au sein des régions et entre elles.

Vous pouvez utiliser les métriques de décompte des règles de réplication S3 Storage Lens pour obtenir des informations détaillées par compartiment sur les compartiments configurés pour la réplication. Ces informations incluent les règles de réplication au sein des compartiments et des régions et entre eux.

Prérequis

Pour voir les métriques de décompte des règles de réplication dans votre tableau de bord S3 Storage Lens, vous devez activer Advanced metrics and recommendations (Métriques et recommandations avancées) de S3 Storage Lens, puis sélectionner Advanced data protection metrics (Métriques avancées sur la protection des données). Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

Étape 1 : compter le nombre total de règles de réplication pour chaque compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans votre tableau de bord Storage Lens, choisissez l'onglet Bucket (Compartiment).

5. Faites défiler jusqu'à la section Buckets (Compartiments). Sous Metrics categories (Catégories de métriques), choisissez Data protection (Protection des données). Effacez ensuite Summary (Résumé).
6. Pour filtrer la liste Buckets (Compartiments) afin d'afficher uniquement les métriques de décompte des règles de réplication, choisissez l'icône des préférences ().
7. Désactivez les boutons bascules pour toutes les métriques sur la protection des données jusqu'à ce que seules les métriques de décompte des règles de réplication restent sélectionnées :
   - Nombre de règles de réplication pour la même région
   - Nombre de règles de réplication entre régions
   - Same-account replication rule count (Nombre de règles de réplication pour le même compte)
   - Cross-account replication rule count (Nombre de règles de réplication entre comptes)
   - Total replication rule count (Nombre total de règles de réplication)
8. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.
9. Choisissez Confirmer.

Étape 2 : ajouter des règles de réplication

Une fois que vous avez déterminé le nombre de règles de réplication par compartiment, vous pouvez éventuellement créer des règles de réplication supplémentaires. Pour de plus amples informations, veuillez consulter Exemples de configuration de la réplication en direct.

Identification du pourcentage d'octets de verrouillage d'objets

Avec S3 Object Lock, vous pouvez stocker des objets à l'aide d'un modèle write-once-read-many (WORM). Vous pouvez utiliser le verrouillage des objets pour empêcher que des objets soient supprimés ou remplacés pendant une durée déterminée ou indéfinie. Vous pouvez activer le verrouillage des objets uniquement lorsque vous créez un compartiment et activez également la gestion des versions S3. Toutefois, vous pouvez modifier la période de rétention pour des versions d'objet individuelles ou appliquer des conservations légales aux compartiments pour lesquels le verrouillage d'objet est activé. Pour de plus amples informations, veuillez consulter Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.

Vous pouvez utiliser les métriques de verrouillage d'objets dans S3 Storage Lens pour voir la métrique % d'octets de verrouillage d'objets pour votre compte ou votre organisation. Vous pouvez utiliser ces informations pour identifier les compartiments de votre compte ou de votre organisation qui ne respectent pas vos bonnes pratiques de protection des données.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans la section Snapshot (Instantané), sous Metrics categories (Catégories de métriques), choisissez Data protection (Protection des données).

   La section Instantané est mise à jour pour afficher les métriques sur la protection des données, notamment la métrique % d'octets de verrouillage d'objets. Vous pouvez voir le pourcentage global d'octets de verrouillage d'objets pour votre compte ou votre organisation.
5. Pour voir la métrique % d'octets de verrouillage d'objets par compartiment, faites défiler la page vers le bas jusqu'à la section Aperçu des N éléments principaux.

   Pour obtenir des données au niveau des objets pour le verrouillage d'objet, vous pouvez également utiliser les métriques Nombre d'objets de verrouillage d'objet et % d'objets de verrouillage d'objet.
6. Pour Métrique, choisissez % d'octets de verrouillage d'objets dans la catégorie Protection des données.

   Par défaut, la section Top N overview for date (Aperçu des N éléments principaux pour date) affiche les métriques des 3 principaux compartiments. Dans le champ Top N (N éléments principaux), vous pouvez augmenter le nombre de compartiments. La section Top N overview for date (Aperçu des N éléments principaux pour date) indique également la variation en pourcentage par rapport à la journée ou à la semaine précédente et une ligne étincelante pour visualiser la tendance. Cette tendance est une tendance sur 14 jours pour les métriques gratuites et une tendance sur 30 jours pour les métriques et recommandations avancées.

> **Note**
>
> Grâce aux métriques et recommandations avancées S3 Storage Lens, les métriques sont disponibles pour les requêtes pendant 15 mois. Pour de plus amples informations, veuillez consulter Sélection des métriques.

7. Passez en revue les données suivantes pour % d'octets de verrouillage d'objets :

   - nombre comptes principaux : découvrez quels comptes ont la métrique % d'octets de verrouillage d'objets la plus élevée et la plus faible.
   - nombre régions principales : affichez une répartition de la métrique % d'octets de verrouillage d'objets par région.
   - nombre compartiments principaux : découvrez quels compartiments ont la métrique % d'octets de verrouillage d'objets la plus élevée et la plus faible.

Utilisation de S3 Storage Lens pour auditer les paramètres de propriété d'objets

Amazon S3 Object Ownership est un paramètre au niveau du compartiment S3 que vous pouvez utiliser pour désactiver les listes de contrôle d'accès (ACLs) et contrôler la propriété des objets de votre compartiment. Si vous définissez Object Ownership comme étant appliqué par le propriétaire du bucket, vous pouvez désactiver les listes de contrôle d'accès (ACLs) et vous approprier tous les objets de votre bucket. Cette approche simplifie la gestion des accès pour les données stockées dans Amazon S3.

Par défaut, lorsqu'un autre Compte AWS utilisateur télécharge un objet dans votre compartiment S3, ce compte (le rédacteur de l'objet) est propriétaire de l'objet, y a accès et peut autoriser d'autres utilisateurs à y accéder par le biais ACLs de ce compte. Vous pouvez utiliser la propriété de l'objet pour modifier ce comportement par défaut.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Par conséquent, nous vous recommandons de le désactiver ACLs, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. En définissant la propriété des objets comme étant appliquée par le propriétaire du compartiment, vous pouvez désactiver les politiques de contrôle d'accès ACLs et vous appuyer sur celles-ci. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

Grâce aux métriques de gestion des accès de S3 Storage Lens, vous pouvez identifier les compartiments qui ne sont pas désactivés. ACLs Après avoir identifié ces compartiments, vous pouvez migrer les autorisations ACL vers des politiques et les désactiver ACLs pour ces compartiments.

Rubriques

- Étape 1 : identifier les tendances générales relatives aux paramètres de propriété d'objets
- Étape 2 : identifier les tendances au niveau du compartiment relatives aux paramètres de propriété d'objets
- Étape 3 : mettre à jour le paramètre de propriété de l'objet pour que le propriétaire du compartiment soit désactivé ACLs

Étape 1 : identifier les tendances générales relatives aux paramètres de propriété d'objets

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans la section Snapshot for date (Instantané pour date), sous Metrics categories (Catégories de métriques), choisissez Access management (Gestion des accès).

   La section Snapshot for date (Instantané pour date) est mise à jour pour afficher la métrique % Object Ownership bucket owner enforced (% de compartiments avec propriété d'objets Appliqué par le propriétaire du compartiment). Vous pouvez voir le pourcentage global de buckets de votre compte ou de votre organisation qui utilisent le paramètre imposé par le propriétaire du bucket pour désactiver ACLs la propriété des objets.

Étape 2 : identifier les tendances au niveau du compartiment relatives aux paramètres de propriété d'objets

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).

3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Pour afficher des métriques plus détaillées au niveau du compartiment, choisissez l'onglet Bucket (Compartiment).
5. Dans la section Distribution by buckets for date (Distribution par compartiments pour date), choisissez la métrique % Object Ownership bucket owner enforced (% de compartiments avec propriété d'objets Appliqué par le propriétaire du compartiment).

   Le graphique est mis à jour pour montrer la répartition par compartiment pour % Object Ownership bucket owner enforced (% de compartiments avec propriété d'objets Appliqué par le propriétaire du compartiment). Vous pouvez voir quels compartiments utilisent le paramètre imposé par le propriétaire du compartiment pour désactiver ACLs la propriété des objets.
6. Pour voir les paramètres Appliqué par le propriétaire du compartiment en contexte, faites défiler l'affichage jusqu'à la section Buckets (Compartiments). Pour Metrics categories (Catégories de métriques), sélectionnez Access management (Gestion des accès). Effacez ensuite Summary (Résumé).

   La liste Buckets (Compartiments) affiche les données relatives aux trois paramètres de propriété d'objets : Appliqué par le propriétaire du compartiment, Préféré par le propriétaire du compartiment et Enregistreur d'objets.
7. Pour filtrer la liste Buckets (Compartiments) afin d'afficher des métriques uniquement pour un paramètre de propriété d'objets spécifique, choisissez l'icône des préférences ( ).
8. Effacez les métriques que vous ne souhaitez pas afficher.
9. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.
10. Choisissez Confirmer.

Étape 3 : mettre à jour le paramètre de propriété de l'objet pour que le propriétaire du compartiment soit désactivé ACLs

Après avoir identifié les compartiments qui utilisent le paramètre de propriété d'objets Enregistreur d'objets ou Préféré par le propriétaire du compartiment, vous pouvez migrer vos autorisations ACL vers des politiques de compartiments. Lorsque vous avez terminé de migrer vos autorisations ACL, vous pouvez mettre à jour vos paramètres de propriété des objets pour que le propriétaire du bucket

soit appliqué afin de les désactiver ACLs. Pour de plus amples informations, veuillez consulter Conditions préalables à la désactivation ACLs.

Utilisation de métriques S3 Storage Lens pour améliorer les performances

Si vous avez activé S3 Storage Lens advanced metrics (Métriques avancées S3 Storage Lens), vous pouvez utiliser des métriques de codes de statut détaillés pour obtenir le nombre de demandes ayant réussi ou échoué. Vous pouvez utiliser ces informations pour résoudre les problèmes d'accès et de performances. Les métriques de codes de statut détaillés indiquent les nombres de codes de statut HTTP, tels que 403 Forbidden et 503 Service non disponible. Vous pouvez examiner les tendances globales pour obtenir les métriques de codes de statut détaillés pour les compartiments, les comptes et les organisations S3. Vous pouvez ensuite explorer les métriques au niveau des compartiments afin d'identifier les charges de travail qui accèdent actuellement à ces compartiments et provoquent des erreurs.

Par exemple, vous pouvez consulter la métrique Nombre d'erreurs 403 Forbidden pour identifier les charges de travail qui accèdent à des compartiments sans appliquer les autorisations appropriées. Après avoir identifié ces charges de travail, vous pouvez effectuer un examen détaillé en dehors de S3 Storage Lens pour résoudre vos erreurs 403 Forbidden.

Cet exemple montre comment effectuer une analyse de tendances pour l'erreur 403 Forbidden à l'aide des métriques Nombre d'erreurs 403 Forbidden et % d'erreurs 403 Forbidden. Vous pouvez utiliser ces métriques pour identifier les charges de travail qui accèdent aux compartiments sans appliquer les autorisations appropriées. Vous pouvez effectuer une analyse de tendances similaire pour n'importe laquelle des autres Detailed status code metrics (métriques de codes de statut détaillés). Pour plus d'informations, consultez Glossaire des métriques Amazon S3 Storage Lens.

Prérequis

Pour voir les Detailed status code metrics (métriques de codes de statut détaillés) dans votre tableau de bord S3 Storage Lens, vous devez activer Advanced metrics and recommendations (Métriques et recommandations avancées) S3 Storage Lens, puis sélectionner Detailed status code metrics (Métriques de codes de statut détaillés). Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

Rubriques

- Étape 1 : réaliser une analyse des tendances pour un code de statut HTTP individuel
- Étape 2 : analyser les nombres d'erreurs par compartiment

- Étape 3 : entreprendre la résolution des erreurs

Étape 1 : réaliser une analyse des tendances pour un code de statut HTTP individuel

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans la section Tendances et distributions, pour Métrique principale, choisissez Nombre d'erreurs 403 Forbidden dans la catégorie Codes de statut détaillés. Pour Métrique secondaire, choisissez % d'erreurs 403 Forbidden .
5. Faites défiler l'écran vers le bas jusqu'à la section Top N overview for date (Aperçu des N éléments principaux pour date). Pour Métriques, choisissez Nombre d'erreurs 403 Forbidden ou % d'erreurs 403 Forbidden dans la catégorie Codes de statut détaillés.

   L'aperçu du Top N pour la section des dates est mis à jour pour afficher les 403 principales erreurs interdites par compte et par compartiment. Région AWS

Étape 2 : analyser les nombres d'erreurs par compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Storage Lens, Dashboards (Tableaux de bord).
3. Dans la liste Dashboards (Tableaux de bord), choisissez le nom du tableau de bord que vous souhaitez afficher.
4. Dans votre tableau de bord Storage Lens, choisissez l'onglet Bucket (Compartiment).
5. Faites défiler jusqu'à la section Buckets (Compartiments). Pour Metrics categories (Catégories de métriques), sélectionnez les métriques Detailed status code (Code de statut détaillé). Effacez ensuite Summary (Résumé).

   La liste Buckets (Compartiments) est mise à jour pour afficher toutes les métriques de code de statut détaillées disponibles. Vous pouvez utiliser ces informations pour voir quels compartiments

contiennent une grande partie de certains codes de statut HTTP et quels codes de statut sont communs à tous les compartiments.

6. Pour filtrer la liste Buckets (Compartiments) afin d'afficher uniquement des métriques de codes de statut détaillés spécifiques, choisissez l'icône des préférences ().
7. Désélectionnez les boutons bascules correspondant à toutes les métriques de codes de statut détaillés que vous ne souhaitez pas afficher dans la liste Buckets (Compartiments).
8. (Facultatif) Sous Page size (Taille de page), choisissez le nombre de compartiments à afficher dans la liste.
9. Choisissez Confirmer.

   La liste Buckets (Compartiments) affiche les métriques des nombres d'erreurs pour le nombre de compartiments que vous avez spécifié. Vous pouvez utiliser ces informations pour identifier les compartiments spécifiques qui rencontrent de nombreuses erreurs et entreprendre la résolution des erreurs par compartiment.

Étape 3 : entreprendre la résolution des erreurs

Après avoir identifié les compartiments présentant une forte proportion de codes de statut HTTP spécifiques, vous pouvez entreprendre la résolution de ces erreurs. Pour plus d'informations, consultez les ressources suivantes :

- Pourquoi est-ce que j'obtiens l'erreur 403 Forbidden quand j'essaie de charger des fichiers dans Amazon S3 ?
- Pourquoi est-ce que j'obtiens l'erreur 403 Forbidden quand j'essaie de modifier une politique de compartiment dans Amazon S3 ?
- Comment résoudre les erreurs 403 Forbidden provenant de mon compartiment Amazon S3 dont toutes les ressources proviennent du même Compte AWS ?
- Comment résoudre une erreur HTTP 500 ou 503 provenant d'Amazon S3 ?

Utilisation d'Amazon S3 Storage Lens avec AWS Organizations

Amazon S3 Storage Lens est une fonction d'analyse du stockage dans le cloud que vous pouvez utiliser pour obtenir une visibilité à l'échelle de l'organisation sur l'utilisation et l'activité du stockage d'objets. Vous pouvez utiliser les métriques S3 Storage Lens pour générer des informations

récapitulatives, telles que la quantité de stockage dont vous disposez dans l'ensemble de votre organisation ou les compartiments et préfixes qui connaissent la croissance la plus rapide. Vous pouvez également utiliser Amazon S3 Storage Lens pour collecter des métriques de stockage et des données d'utilisation pour tous Comptes AWS les éléments de votre AWS Organizations hiérarchie. Pour ce faire, vous devez utiliser AWS Organizations et activer l'accès sécurisé à S3 Storage Lens à l'aide de votre compte AWS Organizations de gestion.

Une fois l'accès approuvé activé, vous pouvez ajouter un accès administrateur délégué aux comptes de votre organisation. Les comptes d'administrateur délégué permettent de créer des configurations et des tableaux de bord S3 Storage Lens qui collectent des métriques de stockage et des données utilisateur à l'échelle de l'organisation. Pour de plus informations sur l'activation d'un accès sécurisé, consultez Amazon S3 Storage Lens et AWS Organizations dans le Guide de l'utilisateur AWS Organizations .

Rubriques

- Activer l'accès sécurisé pour S3 Storage Lens
- Désactiver l'accès sécurisé pour S3 Storage Lens
- Enregistrer un administrateur délégué S3 Storage Lens
- Annuler l'enregistrement d'un administrateur délégué pour S3 Storage Lens

Activer l'accès sécurisé pour S3 Storage Lens

En activant l'accès sécurisé, vous autorisez Amazon S3 Storage Lens à accéder à votre AWS Organizations hiérarchie, à vos membres et à votre structure par le biais d'opérations AWS Organizations d'API. S3 Storage Lens devient alors un service sécurisé pour l'ensemble de la structure de votre organisation.

Chaque fois qu'une configuration de tableau de bord est créée, S3 Storage Lens crée des rôles liés à un service dans les comptes de gestion ou d'administrateur délégué de votre organisation. Le rôle lié à un service accorde à S3 Storage Lens l'autorisation d'effectuer les actions suivantes :

- Décrire les organisations
- Répertorier les comptes
- Vérifier une liste d' Service AWS accès pour les organisations
- Obtenir des administrateurs délégués pour les organisations

S3 Storage Lens peut alors s'assurer qu'il dispose d'un accès pour collecter les métriques intercomptes pour les comptes de votre organisation. Pour plus d'informations, consultez Utilisation des rôles liés à un service pour Amazon S3 Storage Lens.

Une fois l'accès approuvé activé, vous pouvez affecter un accès administrateur délégué aux comptes de votre organisation. Lorsqu'un compte est marqué en tant qu'administrateur délégué pour un service, le compte reçoit l'autorisation d'accéder à toutes les opérations d'API d'organisation en lecture seule. Cet accès fournit une visibilité d'administrateur délégué aux membres et aux structures de votre organisation pour leur permettre à eux aussi de créer des tableaux de bord S3 Storage Lens.

> **Note**
>
> - L'accès sécurisé ne peut être activé que par le compte de gestion.
> - Seuls le compte de gestion et les administrateurs délégués peuvent créer des tableaux de bord ou des configurations S3 Storage Lens pour votre organisation.

Utilisation de la console S3

Pour permettre à S3 Storage Lens de bénéficier d'un accès AWS Organizations sécurisé

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Sélectionnez Paramètres AWS Organizations . La page Accès AWS Organizations pour Storage Lens s'affiche.
4. Sous Accès approuvéAWS Organizations , choisissez Modifier.

   La page Accès AWS Organizations s'affiche.
5. Choisissez Activer pour activer un accès sécurisé pour votre tableau de bord S3 Storage Lens.
6. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

Example

L'exemple suivant vous montre comment activer l'accès AWS Organizations sécurisé pour S3 Storage Lens dans AWS CLI.

```
aws organizations enable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

Utilisation du AWS SDK pour Java

Example — Activez un accès AWS Organizations sécurisé pour S3 Storage Lens à l'aide du SDK for Java

L'exemple suivant illustre comment activer l'accès approuvé pour S3 Storage Lens dans le kit SDK pour Java. Pour utiliser cet exemple, remplacez *`user input placeholders`* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.EnableAWSServiceAccessRequest;

public class EnableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.enableAWSServiceAccess(new
 EnableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
```

```
            e.printStackTrace();
        }
 }
}
```

Désactiver l'accès sécurisé pour S3 Storage Lens

Lorsqu'un compte est supprimé en tant qu'administrateur délégué ou lorsque l'accès approuvé est désactivé, les métriques du tableau de bord S3 Storage Lens du propriétaire du compte fonctionnent uniquement au niveau du compte. Chacun des titulaires de compte ne pourra voir que les avantages de S3 Storage Lens limités à la portée de son compte, et non à celle de toute son organisation.

Lorsque vous désactivez l'accès approuvé dans S3 Storage Lens, les tableaux de bord nécessitant un accès approuvé ne sont plus mis à jour. Les tableaux de bord organisationnels créés ne sont plus mis à jour non plus. Au lieu de cela, vous pouvez uniquement interroger les données historiques du tableau de bord S3 Storage Lens, tant que les données restent disponibles.

> **Note**
>
> - La désactivation de l'accès approuvé pour S3 Storage Lens empêche également automatiquement tous les tableaux de bord au niveau de l'organisation de collecter et d'agréger des métriques de stockage. Cela est dû au fait que S3 Storage Lens ne dispose plus d'un accès approuvé aux comptes de l'organisation.
> - Vos comptes de gestion et d'administrateur délégué peuvent toujours voir les données historiques des tableaux de bord désactivés. Ils peuvent également interroger ces données historiques tant qu'elles sont encore disponibles.

Utilisation de la console S3

Pour désactiver l'accès sécurisé de S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Sélectionnez Paramètres AWS Organizations . La page Accès AWS Organizations pour Storage Lens s'affiche.
4. Sous Accès approuvéAWS Organizations , choisissez Modifier.

La page Accès AWS Organizations s'affiche.

5. Choisissez Désactiver pour désactiver l'accès sécurisé pour votre tableau de bord S3 Storage Lens.
6. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

Example

L'exemple suivant désactive l'accès approuvé pour S3 Storage Lens à l'aide de l' AWS CLI.

```
aws organizations disable-aws-service-access --service-principal storage-
lens.s3.amazonaws.com
```

Utilisation du AWS SDK pour Java

Example — Désactiver l'accès AWS Organizations sécurisé pour S3 Storage Lens

L'exemple suivant montre comment désactiver l'accès AWS Organizations sécurisé pour S3 Storage Lens dans le SDK for Java. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import com.amazonaws.services.organizations.model.DisableAWSServiceAccessRequest;

public class DisableOrganizationsTrustedAccess {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();
```

```
            // Make sure to remove any existing delegated administrator for S3 Storage
 Lens
            // before disabling access; otherwise, the request will fail.
            organizationsClient.disableAWSServiceAccess(new
 DisableAWSServiceAccessRequest()
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

Enregistrer un administrateur délégué S3 Storage Lens

Vous pouvez créer des tableaux de bord au niveau de l'organisation à l'aide des comptes de gestion ou d'administrateur délégué de votre organisation. Les comptes d'administrateur délégué permettent à d'autres comptes que votre compte de gestion de créer des tableaux de bord au niveau de l'organisation. Seul le compte de gestion d'une organisation peut enregistrer et annuler d'autres comptes en tant qu'administrateurs délégués pour l'organisation.

Après avoir activé l'accès sécurisé, vous pouvez enregistrer l'accès administrateur délégué aux comptes de votre organisation à l'aide de l' AWS Organizations API REST ou SDKs à partir du compte de gestion. AWS CLI Pour plus d'informations, consultez RegisterDelegatedAdministrator dans la Référence d'API AWS Organizations . Lorsqu'un compte est enregistré en tant qu'administrateur délégué, il reçoit l'autorisation d'accéder à toutes les opérations d' AWS Organizations API en lecture seule. Cela donne une visibilité aux membres et aux structures de votre organisation, qui peuvent créer des tableaux de bord S3 Storage Lens en votre nom.

> **Note**
>
> Avant de pouvoir désigner un administrateur délégué à l'aide de l' AWS Organizations API REST AWS CLI, ou SDKs, vous devez appeler l'EnableAWSOrganizationsAccessopération.

Utilisation de la console S3

Pour enregistrer des administrateurs délégués pour S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Sélectionnez Paramètres AWS Organizations .
4. Sous Administrateur délégué, sélectionnez Enregistrer un nouveau compte.
5. Ajoutez un Compte AWS identifiant pour enregistrer le compte en tant qu'administrateur délégué. L'administrateur délégué est en mesure de créer des tableaux de bord au niveau de l'organisation pour tous les comptes et le stockage de votre organisation.
6. Choisissez Enregistrer un compte.

En utilisant le AWS CLI

Example

L'exemple suivant illustre comment enregistrer des administrateurs délégués Organizations pour S3 Storage Lens à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
aws organizations register-delegated-administrator --service-principal storage-
lens.s3.amazonaws.com --account-id 111122223333
```

Utilisation du AWS SDK pour Java

Example – Enregistrer des administrateurs délégués Organizations pour S3 Storage Lens

L'exemple suivant montre comment enregistrer des administrateurs AWS Organizations délégués pour S3 Storage Lens dans le SDK for Java. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
```

```
import
 com.amazonaws.services.organizations.model.RegisterDelegatedAdministratorRequest;

public class RegisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();

            organizationsClient.registerDelegatedAdministrator(new
 RegisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

Annuler l'enregistrement d'un administrateur délégué pour S3 Storage Lens

Une fois l'accès approuvé activé, vous pouvez enregistrer un accès administrateur délégué aux comptes de votre organisation. Les comptes d'administrateur délégué permettent à d'autres comptes que votre compte de gestion de créer des tableaux de bord au niveau de l'organisation. Seul le compte de gestion d'une organisation peut désinscrire des comptes en tant qu'administrateurs délégués pour l'organisation.

Vous pouvez désenregistrer un administrateur délégué en utilisant l' AWS Organizations AWS Management Console API REST ou AWS CLI les AWS SDK du compte de gestion. Pour plus

d'informations, consultez DeregisterDelegatedAdministrator dans la Référence d'API AWS Organizations .

Lorsqu'un compte n'est plus enregistré en tant qu'administrateur délégué, il perd l'accès aux éléments suivants :

- Toutes les opérations d' AWS Organizations API en lecture seule qui fournissent de la visibilité aux membres et aux structures de votre organisation.
- Tous les tableaux de bord au niveau de l'organisation créés par l'administrateur délégué. La désinscription d'un administrateur délégué empêche également automatiquement tous les tableaux de bord au niveau de l'organisation créés par cet administrateur délégué d'agréger de nouvelles métriques de stockage.

> **Note**
>
> L'administrateur délégué dont l'enregistrement a été annulé peut toujours consulter les données historiques des tableaux de bord qu'il a créé tant que les données restent disponibles pour les requêtes.

Utilisation de la console S3

Pour annuler l'enregistrement d'administrateurs délégués pour S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, accédez à Storage Lens.
3. Sélectionnez Paramètres AWS Organizations .
4. Sous Administrateurs délégués, sélectionnez le compte dont vous souhaitez annuler l'enregistrement.
5. Choisissez Désenregistrer un compte. Le compte dont l'enregistrement a été annulé n'est plus un administrateur délégué et n'est plus en mesure de créer des tableaux de bord au niveau de l'organisation pour tous les comptes et le stockage de votre organisation.
6. Choisissez Enregistrer un compte.

En utilisant le AWS CLI

Example

L'exemple suivant illustre comment annuler l'enregistrement d'administrateurs délégués Organizations pour S3 Storage Lens à l'aide de l' AWS CLI. Pour utiliser cet exemple, remplacez *111122223333* par l'ID de votre Compte AWS .

```
aws organizations deregister-delegated-administrator --service-principal storage-
lens.s3.amazonaws.com --account-id 111122223333
```

Utilisation du AWS SDK pour Java

Example – Annuler l'enregistrement des administrateurs délégués Organizations pour S3 Storage Lens

L'exemple suivant illustre comment annuler l'enregistrement d'administrateurs délégués Organizations pour S3 Storage Lens à l'aide du kit SDK pour Java. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.organizations.AWSOrganizations;
import com.amazonaws.services.organizations.AWSOrganizationsClient;
import
 com.amazonaws.services.organizations.model.DeregisterDelegatedAdministratorRequest;

public class DeregisterOrganizationsDelegatedAdministrator {
 private static final String S3_STORAGE_LENS_SERVICE_PRINCIPAL = "storage-
lens.s3.amazonaws.com";

 public static void main(String[] args) {
  try {
            String delegatedAdminAccountId = "111122223333"; // Account Id for the
 delegated administrator.
            AWSOrganizations organizationsClient = AWSOrganizationsClient.builder()
                .withCredentials(new ProfileCredentialsProvider())
                .withRegion(Regions.US_EAST_1)
                .build();
```

```
            organizationsClient.deregisterDelegatedAdministrator(new
 DeregisterDelegatedAdministratorRequest()
                .withAccountId(delegatedAdminAccountId)
                .withServicePrincipal(S3_STORAGE_LENS_SERVICE_PRINCIPAL));
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but AWS Organizations couldn't
 process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // AWS Organizations couldn't be contacted for a response, or the client
            // couldn't parse the response from AWS Organizations.
            e.printStackTrace();
        }
 }
}
```

Utilisation des groupes S3 Storage Lens pour filtrer et agréger des métriques

Un groupe Amazon S3 Storage Lens regroupe les métriques à l'aide de filtres personnalisés basés sur les métadonnées des objets. Les groupes Storage Lens vous permettent d'analyser en détail les caractéristiques de vos données, telles que la répartition des objets par âge, les types de fichiers les plus courants, etc. Par exemple, vous pouvez filtrer les métriques par balise d'objet pour identifier les jeux de données dont la croissance est la plus rapide, ou visualiser votre stockage en fonction de la taille et de l'âge des objets pour définir votre stratégie d'archivage de stockage. Ainsi, les groupes Amazon S3 Storage Lens vous aident à mieux comprendre et à optimiser votre stockage S3.

Lorsque vous utilisez des groupes Storage Lens, vous pouvez analyser et filtrer les métriques S3 Storage Lens à l'aide de métadonnées d'objets, telles que les préfixes, les suffixes, les balises d'objet, la taille ou l'âge de l'objet. Vous pouvez également appliquer une combinaison de ces filtres. Après avoir attaché votre groupe Storage Lens à votre tableau de bord S3 Storage Lens, vous pouvez consulter les métriques S3 Storage Lens agrégées par les groupes Amazon S3 Storage Lens directement dans votre tableau de bord.

Par exemple, vous pouvez également filtrer vos métriques par taille d'objet ou par tranche d'âge afin de déterminer quelle partie de votre espace de stockage est constituée de petits objets. Vous pouvez ensuite utiliser ces informations avec S3 Intelligent-Tiering ou S3 Lifecycle pour transférer les petits objets vers différentes classes de stockage afin d'optimiser les coûts et le stockage.

Rubriques

- Fonctionnement des groupes S3 Storage Lens
- Utilisation des groupes Storage Lens

Fonctionnement des groupes S3 Storage Lens

Vous pouvez utiliser les groupes Storage Lens pour regrouper les métriques à l'aide de filtres personnalisés basés sur les métadonnées des objets. Lorsque vous définissez un filtre personnalisé, vous pouvez utiliser des préfixes, des suffixes, des balises d'objet, des tailles d'objets, leur âge ou une combinaison de ces filtres personnalisés. Lors de la création d'un groupe Storage Lens, vous pouvez également inclure un filtre ou plusieurs conditions de filtre. Pour spécifier plusieurs conditions de filtre, utilisez les opérateurs logiques `And` ou `Or`.

Lorsque vous créez et configurez un groupe Storage Lens, le groupe Storage Lens lui-même agit comme un filtre personnalisé dans le tableau de bord auquel vous attachez le groupe. Dans votre tableau de bord, vous pouvez ensuite utiliser le filtre de groupe Storage Lens pour obtenir des métriques de stockage en fonction du filtre personnalisé que vous avez défini dans le groupe.

Pour consulter les données de votre groupe Storage Lens dans votre tableau de bord S3 Storage Lens, vous devez attacher le groupe au tableau de bord après l'avoir créé. Une fois que votre groupe Storage Lens est attaché à votre tableau de bord Storage Lens, celui-ci collecte les statistiques d'utilisation du stockage pendant 48 heures. Vous pouvez ensuite visualiser ces données dans le tableau de bord Storage Lens ou les exporter via une exportation de métriques. Si vous oubliez d'attacher un groupe Storage Lens à un tableau de bord, les données de votre groupe Storage Lens ne seront pas capturées ou ne s'afficheront nulle part.

> **Note**
>
> - Lorsque vous créez un groupe S3 Storage Lens, vous créez une AWS ressource. Par conséquent, chaque groupe Storage Lens possède son propre Amazon Resource Name (ARN), que vous pouvez spécifier lorsque vous l'attachez ou que vous l'excluez d'un tableau de bord S3 Storage Lens.
> - Si votre groupe Storage Lens n'est pas attaché à un tableau de bord, vous n'aurez pas à payer de frais supplémentaires pour créer un groupe Storage Lens.
> - S3 Storage Lens regroupe les métriques d'utilisation d'un objet dans tous les groupes Storage Lens correspondants. Par conséquent, si un objet correspond aux conditions de

filtre pour au moins deux groupes Storage Lens, vous constaterez des décomptes répétés pour le même objet dans l'ensemble de votre utilisation du stockage.

Vous pouvez créer un groupe Storage Lens au niveau du compte dans une région d'origine spécifiée (à partir de la liste des groupes pris en charge Régions AWS). Vous pouvez ensuite attacher votre groupe Storage Lens à plusieurs tableaux de bord Storage Lens, à condition que les tableaux de bord se trouvent dans le même Compte AWS et la même région d'origine. Vous pouvez créer jusqu'à 50 groupes Storage Lens par région d'origine dans chaque Compte AWS.

Vous pouvez créer et gérer des groupes S3 Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) AWS SDKs, ou de l'API REST Amazon S3.

Rubriques

- Affichage des métriques agrégées d'un groupe Storage Lens
- Autorisations pour les groupes Storage Lens
- Configuration des groupes Storage Lens
- AWS balises de ressources
- Exportation de métriques des groupes Storage Lens

Affichage des métriques agrégées d'un groupe Storage Lens

Vous pouvez consulter les métriques agrégées de vos groupes Storage Lens en attachant les groupes à un tableau de bord. Les groupes Storage Lens que vous souhaitez attacher doivent résider dans la région d'origine désignée dans le compte du tableau de bord.

Pour attacher un groupe Storage Lens à un tableau de bord, vous devez le spécifier dans la section Regroupement des groupes Storage Lens de la configuration de votre tableau de bord. Si vous avez plusieurs groupes Storage Lens, vous pouvez filtrer les résultats du Regroupement des groupes Storage Lens de sorte à inclure ou exclure les groupes de votre choix. Pour plus d'informations sur l'attachement de groupes à vos tableaux de bord, consultez the section called "Attachement ou retrait d'un groupe Storage Lens".

Après avoir attaché vos groupes, vous verrez les données d'agrégation supplémentaires du groupe Storage Lens dans votre tableau de bord dans un délai de 48 heures.

> **Note**
>
> Pour consulter les métriques agrégées de votre groupe Storage Lens, vous devez attacher le groupe à un tableau de bord S3 Storage Lens.

Autorisations pour les groupes Storage Lens

Les groupes Storage Lens nécessitent certaines autorisations dans AWS Identity and Access Management (IAM) pour autoriser l'accès aux actions du groupe S3 Storage Lens. Pour accorder ces autorisations, vous pouvez utiliser une politique IAM basée sur l'identité. Vous pouvez attacher cette politique aux utilisateurs, groupes ou rôles IAM pour leur accorder des autorisations. Ces autorisations peuvent inclure la possibilité de créer ou de supprimer des groupes Storage Lens, d'afficher leurs configurations ou de gérer leurs balises.

L'utilisateur ou le rôle IAM auquel vous accordez des autorisations doit appartenir au compte qui a créé ou qui possède le groupe Storage Lens.

Pour utiliser les groupes Storage Lens et consulter les métriques de vos groupes Storage Lens, vous devez d'abord disposer des autorisations appropriées pour utiliser S3 Storage Lens. Pour de plus amples informations, veuillez consulter the section called "Définition des autorisations d'".

Pour créer et gérer des groupes S3 Storage Lens, vous devez disposer des autorisations IAM suivantes, en fonction des opérations que vous souhaitez effectuer :

Action	Autorisations IAM
Créer un nouveau groupe Storage Lens	`s3:CreateStorageLensGroup`
Créer un nouveau groupe Storage Lens avec des balises	`s3:CreateStorageLensGroup` , `s3:TagResource`
Mettre à jour un groupe Storage Lens existant	`s3:UpdateStorageLensGroup`
Renvoyer les détails de la configuration d'un groupe Storage Lens	`s3:GetStorageLensGroup`
Répertorier tous les groupes Storage Lens de votre région d'origine	`s3:ListStorageLensGroups`

Action	Autorisations IAM
Supprimer un groupe Storage Lens	`s3:DeleteStorageLensGroup`
Répertorier les balises qui ont été ajoutées à votre groupe Storage Lens	`s3:ListTagsForResource`
Ajouter ou mettre à jour une balise de groupe Storage Lens pour un groupe Storage Lens existant	`s3:TagResource`
Supprimer une balise d'un groupe Storage Lens	`s3:UntagResource`

Voici un exemple de configuration de votre politique IAM dans le compte qui crée le groupe Storage Lens. Pour utiliser cette politique, remplacez *`us-east-1`* par la région d'origine dans laquelle se trouve votre groupe Storage Lens. Remplacez *`111122223333`* par votre ID de Compte AWS , puis remplacez *`example-storage-lens-group`* par le nom de votre groupe Storage Lens. Pour appliquer ces autorisations à tous les groupes Storage Lens, remplacez *`example-storage-lens-group`* par *`*`*.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EXAMPLE-Statement-ID",
            "Effect": "Allow",
            "Action": [
                "s3:CreateStorageLensGroup",
                "s3:UpdateStorageLensGroup",
                "s3:GetStorageLensGroup",
                "s3:ListStorageLensGroups",
                "s3:DeleteStorageLensGroup,
                "s3:TagResource",
                "s3:UntagResource",
                "s3:ListTagsForResource"
                ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:storage-lens-group/example-storage-lens-group"
        }
```

```
    ]
}
```

Pour plus d'informations sur les autorisations S3 Storage Lens, consultez Définition d'autorisations Amazon S3 Storage Lens. Pour plus d'informations sur le langage des politiques IAM, consultez Politiques, stratégies et autorisations dans Amazon S3.

Configuration des groupes Storage Lens

Nom de groupe S3 Storage Lens

Nous vous recommandons de donner à vos groupes Storage Lens des noms indiquant leur objectif afin que vous puissiez facilement déterminer les groupes que vous souhaitez attacher à vos tableaux de bord. Pour attacher un groupe Storage Lens à un tableau de bord, vous devez spécifier le groupe dans la section Regroupement des groupes Storage Lens de la configuration de votre tableau de bord.

Les noms de groupe Storage Lens doivent être uniques au sein du compte. Ils ne doivent pas dépasser 64 caractères et peuvent uniquement contenir des lettres (a à z, A à Z), des chiffres (0 à 9), des traits d'union (-) et des traits de soulignement (_).

Région d'accueil

La région d'origine est celle Région AWS où votre groupe Storage Lens est créé et maintenu. Votre groupe Storage Lens est créé dans la même région d'origine que votre tableau de bord Amazon S3 Storage Lens. La configuration et les métriques du groupe Storage Lens sont également stockées dans cette région. Vous pouvez créer jusqu'à 50 groupes Storage Lens dans une région d'origine.

Après avoir créé votre groupe Storage Lens, vous ne pouvez pas modifier la région d'origine.

Portée

Pour inclure des objets dans votre groupe Storage Lens, ils doivent être dans la portée de votre tableau de bord Amazon S3 Storage Lens. La portée de votre tableau de bord Storage Lens est déterminée par les compartiments que vous avez inclus dans la Portée du tableau de bord de la configuration de votre tableau de bord S3 Storage Lens.

Vous pouvez utiliser différents filtres pour vos objets afin de définir la portée de votre groupe Storage Lens. Pour afficher ces métriques de groupe Storage Lens dans votre tableau de bord S3 Storage Lens, les objets doivent correspondre aux filtres que vous incluez dans vos groupes Storage

Lens. Supposons, par exemple, que votre groupe Storage Lens inclut des objets dotés du préfixe `marketing` et du suffixe `.png`, mais qu'aucun objet ne correspond à ces critères. Dans ce cas, les métriques de ce groupe Storage Lens ne seront pas générées lors de votre exportation de métriques quotidienne, et aucune métrique de ce groupe ne sera visible dans votre tableau de bord.

Filtres

Vous pouvez utiliser les filtres suivants dans un groupe S3 Storage Lens :

- Préfixes : indique le préfixe des objets inclus, qui est une chaîne de caractères au début du nom de la clé d'objet. Par exemple, la valeur `images` pour le filtre Préfixes inclut les objets dotés de l'un des préfixes suivants : `images/`, `images-marketing` et `images/production`. La longueur maximale d'un préfixe est de 1 024 octets.
- Suffixes : indique le suffixe des objets inclus (par exemple, `.png`, `.jpeg` ou `.csv`). La longueur maximale d'un suffixe est de 1 024 octets.
- Balises d'objet : indique la liste des balises d'objet sur lesquelles vous souhaitez appliquer le filtre. Une clé de balise ne peut pas dépasser 128 caractères Unicode et une valeur de balise ne peut pas dépasser 256 caractères Unicode. Notez que si le champ de valeur de balise de l'objet est laissé vide, les groupes S3 Storage Lens ne font correspondre l'objet qu'aux autres objets dont les valeurs de balise sont également vides.
- Age : indique la tranche d'âge des objets inclus en jours. Seuls les entiers sont pris en charge.
- Taille : indique la plage de tailles des objets inclus en octets. Seuls les entiers sont pris en charge. La valeur maximale autorisée est de 5 To.

Balises d'objet d'un groupe Storage Lens

Vous pouvez créer un groupe Storage Lens comprenant jusqu'à 10 filtres de balises d'objet. L'exemple suivant inclut deux paires clé-valeur de balise d'objet en tant que filtres pour un groupe Storage Lens nommé *`Marketing-Department`*. Pour utiliser cet exemple, remplacez *`Marketing-Department`* par le nom de votre groupe, puis remplacez *`object-tag-key-1`*, *`object-tag-value-1`*, etc. par les paires clé-valeur de balise d'objet sur lesquelles vous souhaitez appliquer le filtre.

```
{
    "Name": "Marketing-Department",
    "Filter": {
     "MatchAnyTag":[
                {
```

```
                    "Key": "object-tag-key-1",
                    "Value": "object-tag-value-1"
                },
                {
                    "Key": "object-tag-key-2",
                    "Value": "object-tag-value-2"
                }
            ]
    }
}
```

Opérateurs logiques (**`And`** ou **`Or`**)

Pour inclure plusieurs conditions de filtre dans votre groupe Storage Lens, vous pouvez utiliser des opérateurs logiques (`And` ou `Or`). Dans l'exemple suivant, le groupe Storage Lens nommé *`Marketing-Department`* possède un opérateur `And` qui contient les filtres `Prefix`, `ObjectAge` et `ObjectSize`. Étant donné qu'un opérateur `And` est utilisé, seuls les objets répondant à toutes ces conditions de filtre seront inclus dans la portée du groupe Storage Lens.

Pour utiliser cet exemple, remplacez *`user input placeholders`* par les valeurs sur lesquelles vous souhaitez appliquer le filtre.

```
{
    "Name": "Marketing-Department",
    "Filter": {
        "And": {
            "MatchAnyPrefix": [
                "prefix-1",
                "prefix-2",
                "prefix-3/sub-prefix-1"
            ],
             "MatchObjectAge": {
                "DaysGreaterThan": 10,
                "DaysLessThan": 60
            },
            "MatchObjectSize": {
                "BytesGreaterThan": 10,
                "BytesLessThan": 60
            }
        }
    }
}
```

> **Note**
>
> Si vous souhaitez inclure des objets répondant à l'une des conditions des filtres, remplacez l'opérateur logique `And` par l'opérateur logique `Or` dans cet exemple.

AWS balises de ressources

Chaque groupe S3 Storage Lens est considéré comme une AWS ressource dotée de son propre Amazon Resource Name (ARN). Par conséquent, lorsque vous configurez votre groupe Storage Lens, vous pouvez éventuellement ajouter des balises de ressource AWS au groupe. Vous pouvez ajouter jusqu'à 50 balises par groupe Storage Lens. Pour créer un groupe Storage Lens avec des balises, vous devez disposer des autorisations `s3:CreateStorageLensGroup` et `s3:TagResource`.

Vous pouvez utiliser AWS des balises de ressources pour classer les ressources par département, secteur d'activité ou projet. Cela est utile lorsque vous avez de nombreuses ressources du même type. En appliquant des balises, vous pouvez rapidement identifier un groupe Storage Lens spécifique en fonction des balises que vous lui avez affectées. Vous pouvez également utiliser des balises pour suivre et répartir les coûts.

En outre, lorsque vous ajoutez une balise de AWS ressource à votre groupe Storage Lens, vous activez le contrôle d'accès basé sur les attributs (ABAC). L'ABAC est une stratégie d'autorisation qui définit les autorisations en fonction des attributs, dans ce cas, des balises. Vous pouvez également utiliser des conditions qui spécifient des balises de ressources dans vos politiques IAM pour contrôler l'accès aux AWS ressources.

Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. En outre, tenez compte des limitations suivantes :

- Les clés de balise et valeurs de balise sont sensibles à la casse.
- Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur.
- Si vous supprimez une ressource, ses balises sont également supprimées.
- N'incluez pas de données privées ou sensibles dans vos balises de AWS ressources.
- Les balises système (balises dont les clés de balise commencent par `aws:`) ne sont pas prises en charge.

- La longueur de chaque clé de balise ne peut pas dépasser 128 caractères. La longueur de chaque valeur de balise ne peut pas dépasser 256 caractères.

Exportation de métriques des groupes Storage Lens

Les métriques de groupe S3 Storage Lens sont incluses dans l'exportation des métriques Amazon S3 Storage Lens pour le tableau de bord auquel le groupe Storage Lens est attaché. Pour obtenir des informations générales sur la fonctionnalité d'exportation des métriques Storage Lens, consultez Afficher les métriques Amazon S3 Storage Lens à l'aide d'une exportation de données.

Votre exportation de métriques pour les groupes Storage Lens incluent toute métrique S3 Storage Lens dans la portée du tableau de bord auquel le groupe Storage Lens est attaché. L'exportation inclut également des données de métriques supplémentaires pour les groupes Storage Lens.

Une fois que vous avez créé votre groupe Storage Lens, votre exportation de métriques est envoyée quotidiennement au compartiment que vous avez sélectionné lorsque vous avez configuré l'exportation de métriques pour le tableau de bord auquel votre groupe est attaché. La réception de la première exportation de métriques peut prendre jusqu'à 48 heures.

Pour générer des métriques lors de l'exportation quotidienne, les objets doivent correspondre aux filtres que vous incluez dans vos groupes Storage Lens. Si aucun objet ne correspond aux filtres que vous avez inclus dans votre groupe Storage Lens, aucune métrique ne sera générée. Toutefois, si un objet correspond à au moins deux groupes Storage Lens, l'objet est répertorié séparément pour chaque groupe lorsqu'il apparaît dans l'exportation de métriques.

Vous pouvez identifier les métriques pour les groupes Storage Lens en recherchant l'une des valeurs suivantes dans la colonne `record_type` de l'exportation de métriques pour votre tableau de bord :

- `STORAGE_LENS_GROUP_BUCKET`
- `STORAGE_LENS_GROUP_ACCOUNT`

La colonne `record_value` affiche l'ARN de ressource du groupe Storage Lens (par exemple, `arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-Department`).

Utilisation des groupes Storage Lens

Les groupes Amazon S3 Storage Lens regroupent les métriques à l'aide de filtres personnalisés basés sur les métadonnées des objets. Vous pouvez analyser et filtrer les métriques S3 Storage Lens

à l'aide de préfixes, suffixes, balises d'objet, taille ou âge d'objet. Les groupes Amazon S3 Storage Lens vous permettent également de classer votre utilisation au sein des compartiments Amazon S3 et entre eux. Ainsi, vous serez en mesure de mieux comprendre et d'optimiser votre stockage S3.

Pour commencer à visualiser les données d'un groupe Storage Lens, vous devez d'abord attacher votre groupe Storage Lens à un tableau de bord S3 Storage Lens. Si vous devez gérer des groupes Storage Lens dans le tableau de bord, vous pouvez modifier la configuration du tableau de bord. Pour vérifier quels groupes Storage Lens sont associés à votre compte, vous pouvez les répertorier. Pour vérifier quels groupes Storage Lens sont attachés à votre tableau de bord, vous pouvez toujours consulter l'onglet Groupes Storage Lens du tableau de bord. Pour consulter ou mettre à jour la portée d'un groupe Storage Lens existant, vous pouvez consulter ses détails. Vous pouvez également supprimer définitivement un groupe Storage Lens.

Pour gérer les autorisations, vous pouvez créer et ajouter des balises de AWS ressources définies par l'utilisateur à vos groupes Storage Lens. Vous pouvez utiliser AWS des balises de ressources pour classer les ressources par département, secteur d'activité ou projet. Cela est utile lorsque vous avez de nombreuses ressources du même type. En appliquant des balises, vous pouvez rapidement identifier un groupe Storage Lens spécifique en fonction des balises que vous lui avez affectées.

En outre, lorsque vous ajoutez une balise de AWS ressource à votre groupe Storage Lens, vous activez le contrôle d'accès basé sur les attributs (ABAC). L'ABAC est une stratégie d'autorisation qui définit les autorisations en fonction des attributs, dans ce cas, des balises. Vous pouvez également utiliser des conditions qui spécifient des balises de ressources dans vos politiques IAM pour contrôler l'accès aux AWS ressources.

Rubriques

- Création d'un groupe Storage Lens
- Attachement ou retrait de groupes S3 Storage Lens à ou de votre tableau de bord
- Visualisation des données de vos groupes Storage Lens
- Mise à jour d'un groupe Storage Lens
- Gestion des balises de AWS ressources avec les groupes Storage Lens
- Liste de tous les groupes Storage Lens
- Affichage des détails d'un groupe Storage Lens
- Suppression d'un groupe Storage Lens

Création d'un groupe Storage Lens

Les exemples suivants montrent comment créer un groupe Amazon S3 Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour créer un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, sélectionnez le nom de la région AWS actuellement affichée. Choisissez ensuite la région à laquelle vous souhaitez passer.
3. Dans le volet de navigation de gauche, choisissez Groupes Storage Lens.
4. Choisissez Créer un groupe Storage Lens.
5. Sous Général, affichez votre région d'origine et entrez le nom de votre groupe Storage Lens.
6. Sous Portée, choisissez le filtre que vous souhaitez appliquer à votre groupe Storage Lens. Pour appliquer plusieurs filtres, choisissez vos filtres, puis l'opérateur logique AND ou OR.
   - Pour le filtre Préfixes, choisissez Préfixes et entrez une chaîne de préfixe. Pour ajouter plusieurs préfixes, choisissez Ajouter un préfixe. Pour supprimer un préfixe, choisissez Supprimer en regard du préfixe que vous souhaitez supprimer.
   - Pour le filtre Balises d'objet, choisissez Balises d'objet et entrez la paire clé-valeur de votre objet. Choisissez ensuite Ajouter une balise. Pour supprimer une balise, choisissez Supprimer en regard de la balise que vous souhaitez supprimer.
   - Pour le filtre Suffixes, choisissez Suffixes et entrez une chaîne de suffixe. Pour ajouter plusieurs suffixes, choisissez Ajouter un suffixe. Pour supprimer un suffixe, choisissez Supprimer en regard du suffixe que vous souhaitez supprimer.
   - Pour le filtre Age, spécifiez la tranche d'âge de l'objet en jours. Choisissez Spécifier l'âge minimum de l'objet, puis entrez l'âge minimal de l'objet. Choisissez ensuite Spécifier l'âge maximum de l'objet, puis entrez l'âge maximal de l'objet.
   - Pour le filtre Taille, spécifiez la plage de tailles de l'objet et l'unité de mesure. Choisissez Spécifier la taille minimale d'objet, puis entrez la taille minimale de l'objet. Choisissez Spécifier la taille maximale d'objet, puis entrez la taille maximale de l'objet.
7. (Facultatif) Pour les balises de AWS ressources, ajoutez la paire clé-valeur, puis choisissez Ajouter une balise.

8. Choisissez Créer un groupe Storage Lens.

En utilisant le AWS CLI

L'exemple de AWS CLI commande suivant crée un groupe Storage Lens. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

L'exemple de AWS CLI commande suivant crée un groupe Storage Lens avec deux balises de AWS ressources. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control create-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json \
--tags Key=k1,Value=v1 Key=k2,Value=v2
```

Pour obtenir des exemples de configuration JSON, consultez Configuration des groupes Storage Lens.

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant crée un groupe Storage Lens. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

Example – Création d'un groupe Storage Lens avec un seul filtre

L'exemple suivant crée un groupe Storage Lens nommé *Marketing-Department*. Ce groupe possède un filtre d'âge d'objet qui spécifie la tranche d'âge sur *30* à *90* jours. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
```

```
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;

public class CreateStorageLensGroupWithObjectAge {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupFilter objectAgeFilter = StorageLensGroupFilter.builder()
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90)
                            .build())
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(objectAgeFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – Création d'un groupe Storage Lens avec un opérateur **AND** incluant plusieurs filtres

L'exemple suivant crée un groupe Storage Lens nommé *Marketing-Department*. Ce groupe utilise l'opérateur AND pour indiquer que les objets doivent correspondre à toutes les conditions de filtre. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectAge;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.S3Tag;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupAndOperator;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;


public class CreateStorageLensGroupWithAndFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create object tags.
            S3Tag tag1 = S3Tag.builder()
                    .key("object-tag-key-1")
                    .value("object-tag-value-1")
                    .build();
            S3Tag tag2 = S3Tag.builder()
                    .key("object-tag-key-2")
                    .value("object-tag-value-2")
                    .build();

            StorageLensGroupAndOperator andOperator =
 StorageLensGroupAndOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchAnySuffix(".png", ".gif", ".jpg")
```

```
                    .matchAnyTag(tag1, tag2)
                    .matchObjectAge(MatchObjectAge.builder()
                            .daysGreaterThan(30)
                            .daysLessThan(90).build())
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L).build())
                    .build();

            StorageLensGroupFilter andFilter = StorageLensGroupFilter.builder()
                    .and(andOperator)
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(andFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – Création d'un groupe Storage Lens avec un opérateur **OR** incluant plusieurs filtres

L'exemple suivant crée un groupe Storage Lens nommé *Marketing-Department*. Ce groupe utilise un opérateur OR pour appliquer un filtre de préfixe (*prefix-1*, *prefix-2*, *prefix3/sub-prefix-1*) ou un filtre de taille d'objet avec une plage de tailles comprise entre *1000* octets et *6000* octets. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.MatchObjectSize;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupOrOperator;

public class CreateStorageLensGroupWithOrFilter {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            StorageLensGroupOrOperator orOperator =
 StorageLensGroupOrOperator.builder()
                    .matchAnyPrefix("prefix-1", "prefix-2", "prefix-3/sub-prefix-1")
                    .matchObjectSize(MatchObjectSize.builder()
                            .bytesGreaterThan(1000L)
                            .bytesLessThan(6000L)
                            .build())
                    .build();

            StorageLensGroupFilter orFilter = StorageLensGroupFilter.builder()
                    .or(orOperator)
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(orFilter)
```

```
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example — Créez un groupe Storage Lens avec un seul filtre et deux balises de AWS ressources

L'exemple suivant crée un groupe Storage Lens nommé *Marketing-Department* qui possède un filtre de suffixe. Cet exemple ajoute également deux balises de AWS ressources au groupe Storage Lens. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.CreateStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.Tag;
```

```
public class CreateStorageLensGroupWithResourceTags {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create AWS resource tags.
            Tag resourceTag1 = Tag.builder()
                    .key("resource-tag-key-1")
                    .value("resource-tag-value-1")
                    .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-value-2")
                    .build();

            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            CreateStorageLensGroupRequest createStorageLensGroupRequest =
 CreateStorageLensGroupRequest.builder()
                    .storageLensGroup(storageLensGroup)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId).build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.createStorageLensGroup(createStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
```

```
        }
    }
}
```

Pour obtenir des exemples de configuration JSON, consultez Configuration des groupes Storage Lens.

Attachement ou retrait de groupes S3 Storage Lens à ou de votre tableau de bord

Une fois que vous êtes passé au niveau avancé dans Amazon S3 Storage Lens, vous pouvez attacher un groupe Storage Lens à votre tableau de bord. Si vous avez plusieurs groupes Storage Lens, vous pouvez inclure ou exclure les groupes de votre choix.

Vos groupes Storage Lens doivent résider dans la région d'origine désignée dans le compte du tableau de bord. Une fois que vous avez attaché un groupe Storage Lens à votre tableau de bord, vous recevrez les données d'agrégation supplémentaires du groupe Storage Lens dans votre exportation de métriques dans un délai de 48 heures.

> **Note**
>
> Si vous souhaitez consulter les métriques agrégées de votre groupe Storage Lens, vous devez les attacher à votre tableau de bord Storage Lens. Pour obtenir des exemples de fichiers de configuration JSON pour le groupe Storage Lens, consultez Exemple de configuration S3 Storage Lens avec des groupes Storage Lens dans JSON.

Utilisation de la console S3

Pour attacher un groupe Storage Lens à un tableau de bord Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, sous Storage Lens, choisissez Tableaux de bord.
3. Choisissez le bouton d'option du tableau de bord Storage Lens auquel vous souhaitez attacher un groupe Storage Lens.
4. Choisissez Modifier.
5. Sous Metrics selection (Sélection des métriques), choisissez Advanced metrics and recommendations (Métriques et recommandations avancées).

6. Sélectionnez Regroupement des groupes Storage Lens.

> **Note**
>
> Par défaut, Métriques avancées est également sélectionné. Toutefois, vous pouvez également désélectionner ce paramètre, car il n'est pas obligatoire pour agréger les données des groupes Storage Lens.

7. Faites défiler la page jusqu'à Regroupement des groupes Storage Lens et spécifiez le ou les groupes Storage Lens que vous souhaitez inclure ou exclure dans l'agrégation de données. Vous pouvez utiliser les options de filtrage suivantes :

   - Si vous souhaitez inclure certains groupes Storage Lens, choisissez Inclure les groupes Storage Lens. Sous Groupes Storage Lens à inclure, sélectionnez vos groupes Storage Lens.
   - Si vous souhaitez inclure tous les groupes Storage Lens, sélectionnez Inclure tous les groupes Storage Lens de la région d'origine de ce compte.
   - Si vous souhaitez exclure certains groupes Storage Lens, choisissez Exclure les groupes Storage Lens. Sous Groupes Storage Lens à exclure, sélectionnez les groupes Storage Lens que vous souhaitez exclure.

8. Sélectionnez Enregistrer les modifications. Si vous avez configuré vos groupes Storage Lens correctement, vous verrez les données d'agrégation supplémentaires du groupe Storage Lens dans votre tableau de bord dans un délai de 48 heures.

Pour retirer un groupe Storage Lens d'un tableau de bord S3 Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, sous Storage Lens, choisissez Tableaux de bord.
3. Choisissez le bouton d'option du tableau de bord Storage Lens duquel vous souhaitez retirer un groupe Storage Lens.
4. Choisissez Afficher la configuration du tableau de bord.
5. Choisissez Modifier.
6. Faites défiler la page jusqu'à la section Sélection des métriques.
7. Sous Regroupement des groupes Storage Lens, cliquez sur le X en regard du groupe Storage Lens que vous souhaitez retirer. Votre groupe Storage Lens est retiré.

Si vous avez inclus tous vos groupes Storage Lens dans votre tableau de bord, décochez la case en regard de Inclure tous les groupes Storage Lens de la région d'origine de ce compte.

8. Sélectionnez Enregistrer les modifications.

> **Note**
>
> La répercussion des mises à jour de configuration dans votre tableau de bord prend jusqu'à 48 heures.

Utilisation du AWS SDK pour Java

Example – Attacher tous les groupes Storage Lens à un tableau de bord

L'exemple de SDK pour Java suivant associe tous les groupes Storage Lens du *111122223333* compte au tableau *DashBoardConfigurationId* de bord :

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWithStorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel();
```

```
            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – Attacher deux groupes Storage Lens à un tableau de bord

L' AWS SDK pour Java exemple suivant associe deux groupes Storage Lens (*StorageLensGroupName1*et*StorageLensGroupName2*) au *ExampleDashboardConfigurationId* tableau de bord.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
```

```
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroups {
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
 StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
 + ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();
```

```
            s3ControlClient.putStorageLensConfiguration(new
 PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Example – Attacher tous les groupes Storage Lens avec des exclusions

L'exemple de SDK pour Java suivant associe tous les groupes Storage Lens au tableau de bord, à *ExampleDashboardConfigurationId* l'exception des deux spécifiés *StorageLensGroupName1* (*StorageLensGroupName2*et) :

```
package aws.example.s3control;


import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;
import com.amazonaws.services.s3control.model.AccountLevel;
import com.amazonaws.services.s3control.model.BucketLevel;
import com.amazonaws.services.s3control.model.PutStorageLensConfigurationRequest;
import com.amazonaws.services.s3control.model.StorageLensConfiguration;
import com.amazonaws.services.s3control.model.StorageLensGroupLevel;
import com.amazonaws.services.s3control.model.StorageLensGroupLevelSelectionCriteria;

import static com.amazonaws.regions.Regions.US_WEST_2;

public class CreateDashboardWith2StorageLensGroupsExcluded {
```

```
    public static void main(String[] args) {
        String configurationId = "ExampleDashboardConfigurationId";
        String storageLensGroupName1 = "StorageLensGroupName1";
        String storageLensGroupName2 = "StorageLensGroupName2";
        String sourceAccountId = "111122223333";

        try {
            StorageLensGroupLevelSelectionCriteria selectionCriteria = new
StorageLensGroupLevelSelectionCriteria()
                    .withInclude(
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName1,
                            "arn:aws:s3:" + US_WEST_2.getName() + ":" + sourceAccountId
+ ":storage-lens-group/" + storageLensGroupName2);

            System.out.println(selectionCriteria);
            StorageLensGroupLevel storageLensGroupLevel = new StorageLensGroupLevel()
                    .withSelectionCriteria(selectionCriteria);

            AccountLevel accountLevel = new AccountLevel()
                    .withBucketLevel(new BucketLevel())
                    .withStorageLensGroupLevel(storageLensGroupLevel);

            StorageLensConfiguration configuration = new StorageLensConfiguration()
                    .withId(configurationId)
                    .withAccountLevel(accountLevel)
                    .withIsEnabled(true);

            AWSS3Control s3ControlClient = AWSS3ControlClient.builder()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(US_WEST_2)
                    .build();

            s3ControlClient.putStorageLensConfiguration(new
PutStorageLensConfigurationRequest()
                    .withAccountId(sourceAccountId)
                    .withConfigId(configurationId)
                    .withStorageLensConfiguration(configuration)
            );
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
```

```
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Visualisation des données de vos groupes Storage Lens

Vous pouvez visualiser les données de vos groupes Storage Lens en attachant le groupe à votre tableau de bord Amazon S3 Storage Lens. Une fois que vous avez inclus le groupe Storage Lens dans l'agrégation de groupes Storage Lens de la configuration de votre tableau de bord, l'affichage des données du groupe Storage Lens dans votre tableau de bord peut prendre jusqu'à 48 heures.

Une fois la configuration du tableau de bord mise à jour, tous les groupes Storage Lens récemment attachés apparaissent dans la liste des ressources disponibles sous l'onglet Groupes Storage Lens. Vous pouvez également analyser en détail l'utilisation du stockage dans votre onglet Aperçu en découpant les données selon une autre dimension. Par exemple, vous pouvez choisir l'un des éléments répertoriés dans les 3 principales catégories et choisir Analyser par pour découper les données selon une autre dimension. Vous ne pouvez pas appliquer la même dimension que le filtre lui-même.

> **Note**
>
> Vous ne pouvez pas appliquer un filtre de groupe Storage Lens en même temps qu'un filtre de préfixe, ou inversement. Vous ne pouvez pas non plus approfondir l'analyse d'un groupe Storage Lens à l'aide d'un filtre de préfixe.

Vous pouvez utiliser l'onglet Groupes Storage Lens du tableau de bord Amazon S3 Storage Lens pour personnaliser la visualisation des données pour les groupes Storage Lens attachés à votre tableau de bord. Vous pouvez visualiser les données de certains groupes Storage Lens attachés à votre tableau de bord ou de tous les groupes.

Lorsque vous visualisez les données d'un groupe Storage Lens dans votre tableau de bord S3 Storage Lens, tenez compte des points suivants :

- S3 Storage Lens regroupe les métriques d'utilisation d'un objet dans tous les groupes Storage Lens correspondants. Par conséquent, si un objet correspond aux conditions de filtre pour au moins

deux groupes Storage Lens, vous constaterez des décomptes répétés pour le même objet dans l'ensemble de votre utilisation du stockage.

- Les objets doivent correspondre aux filtres que vous incluez dans vos groupes Storage Lens. Si aucun objet ne correspond aux filtres que vous incluez dans votre groupe Storage Lens, aucune métrique n'est générée. Pour déterminer s'il existe des objets non affectés, vérifiez le nombre total d'objets dans le tableau de bord au niveau du compte et au niveau du compartiment.

Mise à jour d'un groupe Storage Lens

Les exemples suivants montrent comment mettre à jour un groupe Amazon S3 Storage Lens. Vous pouvez mettre à jour un groupe Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour mettre à jour un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Groupes Storage Lens.
3. Sous Groupes Storage Lens, choisissez le groupe Storage Lens que vous souhaitez mettre à jour.
4. Sous Portée, choisissez Modifier.
5. Sur la page Portée, sélectionnez le filtre que vous souhaitez appliquer à votre groupe Storage Lens. Pour appliquer plusieurs filtres, sélectionnez vos filtres et choisissez l'opérateur logique AND ou OR.

    - Pour le filtre Préfixes, sélectionnez Préfixes et entrez une chaîne de préfixe. Pour ajouter plusieurs préfixes, choisissez Ajouter un préfixe. Pour supprimer un préfixe, choisissez Supprimer en regard du préfixe que vous souhaitez supprimer.
    - Pour le filtre Balises d'objet, entrez la paire clé-valeur de votre objet. Choisissez ensuite Ajouter une balise. Pour supprimer une balise, choisissez Supprimer en regard de la balise que vous souhaitez supprimer.
    - Pour le filtre Suffixes, sélectionnez Suffixes et entrez une chaîne de suffixe. Pour ajouter plusieurs suffixes, choisissez Ajouter un suffixe. Pour supprimer un suffixe, choisissez Supprimer en regard du suffixe que vous souhaitez supprimer.

- Pour le filtre Age, spécifiez la tranche d'âge de l'objet en jours. Choisissez Spécifier l'âge minimum de l'objet, puis entrez l'âge minimal de l'objet. Pour Spécifier l'âge maximum de l'objet, entrez l'âge maximal de l'objet.
- Pour le filtre Taille, spécifiez la plage de tailles de l'objet et l'unité de mesure. Choisissez Spécifier la taille minimale d'objet, puis entrez la taille minimale de l'objet. Pour Spécifier la taille maximale d'objet, entrez la taille maximale de l'objet.

6. Sélectionnez Enregistrer les modifications. La page de détails du groupe Storage Lens s'affiche.
7. (Facultatif) Si vous souhaitez ajouter une nouvelle balise de AWS ressource, accédez à la section AWS des balises de ressource, puis choisissez Ajouter des balises. La page Ajouter des balises s'affiche.

   Ajoutez la nouvelle paire clé-valeur, puis choisissez Enregistrer les modifications. La page de détails du groupe Storage Lens s'affiche.
8. (Facultatif) Si vous souhaitez supprimer une balise de AWS ressource existante, accédez à la section AWS des balises de ressource, puis sélectionnez la balise de ressource. Ensuite, choisissez Supprimer. La boîte de dialogue Supprimer les balises AWS s'affiche.

   Choisissez à nouveau Supprimer pour supprimer définitivement la balise de ressource AWS .

   > **Note**
   >
   > Une fois que vous avez définitivement supprimé une balise de AWS ressource, elle ne peut pas être restaurée.

En utilisant le AWS CLI

L' AWS CLI exemple de commande suivant renvoie les détails de configuration d'un groupe Storage Lens nommé*marketing-department*. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

L' AWS CLI exemple suivant met à jour un groupe Storage Lens. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control update-storage-lens-group --account-id 111122223333 \
--region us-east-1 --storage-lens-group=file://./marketing-department.json
```

Pour obtenir des exemples de configuration JSON, consultez Configuration des groupes Storage Lens.

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant renvoie les détails de configuration du groupe *Marketing-Department* Storage Lens du compte*111122223333*. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
```

```
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

L'exemple suivant met à jour le groupe Storage Lens nommé *Marketing-Department* dans le compte *111122223333*. Cet exemple met à jour la portée du tableau de bord de sorte à inclure les objets correspondant à l'un des suffixes suivants : *.png*, *.gif*, *.jpg* ou *.jpeg*. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.StorageLensGroup;
import software.amazon.awssdk.services.s3control.model.StorageLensGroupFilter;
import software.amazon.awssdk.services.s3control.model.UpdateStorageLensGroupRequest;

public class UpdateStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            // Create updated filter.
            StorageLensGroupFilter suffixFilter = StorageLensGroupFilter.builder()
                    .matchAnySuffix(".png", ".gif", ".jpg", ".jpeg")
                    .build();

            StorageLensGroup storageLensGroup = StorageLensGroup.builder()
                    .name(storageLensGroupName)
                    .filter(suffixFilter)
                    .build();

            UpdateStorageLensGroupRequest updateStorageLensGroupRequest =
 UpdateStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
```

```
                    .storageLensGroup(storageLensGroup)
                    .accountId(accountId)
                    .build();

            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.updateStorageLensGroup(updateStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Pour obtenir des exemples de configuration JSON, consultez Configuration des groupes Storage Lens.

Gestion des balises de AWS ressources avec les groupes Storage Lens

Chaque groupe Amazon S3 Storage Lens est considéré comme une AWS ressource dotée de son propre Amazon Resource Name (ARN). Par conséquent, lorsque vous configurez votre groupe Storage Lens, vous pouvez éventuellement ajouter des balises de ressource AWS au groupe. Vous pouvez ajouter jusqu'à 50 balises par groupe Storage Lens. Pour créer un groupe Storage Lens avec des balises, vous devez disposer des autorisations `s3:CreateStorageLensGroup` et `s3:TagResource`.

Vous pouvez utiliser AWS des balises de ressources pour classer les ressources par département, secteur d'activité ou projet. Cela est utile lorsque vous avez de nombreuses ressources du même type. En appliquant des balises, vous pouvez rapidement identifier un groupe Storage Lens spécifique en fonction des balises que vous lui avez affectées. Vous pouvez également utiliser des balises pour suivre et répartir les coûts.

En outre, lorsque vous ajoutez une balise de AWS ressource à votre groupe Storage Lens, vous activez le contrôle d'accès basé sur les attributs (ABAC). L'ABAC est une stratégie d'autorisation qui définit les autorisations en fonction des attributs, dans ce cas, des balises. Vous pouvez également

utiliser des conditions qui spécifient des balises de ressources dans vos politiques IAM pour contrôler l'accès aux AWS ressources.

Vous pouvez modifier les clés et valeurs de balise, et vous pouvez retirer des balises d'une ressource à tout moment. En outre, tenez compte des limitations suivantes :

- Les clés de balise et valeurs de balise sont sensibles à la casse.
- Si vous ajoutez une balise ayant la même clé qu'une balise existante sur cette ressource, la nouvelle valeur remplace l'ancienne valeur.
- Si vous supprimez une ressource, ses balises sont également supprimées.
- N'incluez pas de données privées ou sensibles dans vos balises de AWS ressources.
- Les balises système (dont les clés de balise commencent par `aws:`) ne sont pas prises en charge.
- La longueur de chaque clé de balise ne peut pas dépasser 128 caractères. La longueur de chaque valeur de balise ne peut pas dépasser 256 caractères.

Les exemples suivants montrent comment utiliser les balises de AWS ressources avec les groupes Storage Lens.

Rubriques

- Ajouter une balise AWS de ressource à un groupe Storage Lens
- Mise à jour des valeurs de balise d'un groupe Storage Lens
- Supprimer une balise de AWS ressource d'un groupe Storage Lens
- Liste des balises du groupe Storage Lens

Ajouter une balise AWS de ressource à un groupe Storage Lens

Les exemples suivants montrent comment ajouter AWS des balises de ressources à un groupe Amazon S3 Storage Lens. Vous pouvez ajouter des balises de ressources à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour ajouter une balise de AWS ressource à un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Groupes Storage Lens.

3. Sous Groupes Storage Lens, choisissez le groupe Storage Lens que vous souhaitez mettre à jour.
4. Sous Balises de ressources AWS , choisissez Ajouter des balises.
5. Sur la page Ajouter des balises, ajoutez la nouvelle paire clé-valeur.

> **Note**
>
> L'ajout d'une nouvelle balise ayant la même clé qu'une balise existante remplace la valeur de balise précédente.

6. (Facultatif) Pour ajouter plusieurs nouvelles balises, choisissez à nouveau Ajouter une balise pour continuer à ajouter de nouvelles entrées. Vous pouvez ajouter jusqu'à 50 balises de AWS ressources à votre groupe Storage Lens.
7. (Facultatif) Si vous souhaitez retirer une entrée récemment ajoutée, choisissez Retirer en regard de la balise que vous souhaitez retirer.
8. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

L'exemple de AWS CLI commande suivant ajoute deux balises de ressources à un groupe Storage Lens existant nommé*marketing-department*. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v1 Key=k2,Value=v2
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant ajoute deux balises de AWS ressources à un groupe Storage Lens existant. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
```

```
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class TagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            Tag resourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-value-1")
                .build();
            Tag resourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tags(resourceTag1, resourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Mise à jour des valeurs de balise d'un groupe Storage Lens

Les exemples suivants montrent comment mettre à jour les valeurs des balises de groupe Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour mettre à jour une balise de AWS ressource pour un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Groupes Storage Lens.
3. Sous Groupes Storage Lens, choisissez le groupe Storage Lens que vous souhaitez mettre à jour.
4. Sous Balises de ressources AWS , sélectionnez la balise que vous souhaitez mettre à jour.
5. Ajoutez la nouvelle valeur de balise en utilisant la même clé que la paire clé-valeur que vous souhaitez mettre à jour. Cliquez sur l'icône représentant une coche pour mettre à jour la valeur de balise.

   > **Note**
   >
   > L'ajout d'une nouvelle balise ayant la même clé qu'une balise existante remplace la valeur de balise précédente.

6. (Facultatif) Si vous souhaitez ajouter de nouvelles balises, choisissez Ajouter une balise pour ajouter de nouvelles entrées. La page Ajouter des balises s'affiche.

   Vous pouvez ajouter jusqu'à 50 balises de AWS ressources pour votre groupe Storage Lens. Lorsque vous avez terminé d'ajouter des nouvelles balises, choisissez Enregistrer les modifications.
7. (Facultatif) Si vous souhaitez retirer une entrée récemment ajoutée, choisissez Retirer en regard de la balise que vous souhaitez retirer. Lorsque vous avez terminé de retirer des balises, choisissez Enregistrer les modifications.

En utilisant le AWS CLI

L'exemple de AWS CLI commande suivant met à jour deux valeurs de balise pour le groupe Storage Lens nommé*marketing-department*. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control tag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1 --tags Key=k1,Value=v3 Key=k2,Value=v4
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant met à jour les valeurs de deux balises de groupe Storage Lens. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.Tag;
import software.amazon.awssdk.services.s3control.model.TagResourceRequest;

public class UpdateTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            Tag updatedResourceTag1 = Tag.builder()
                .key("resource-tag-key-1")
                .value("resource-tag-updated-value-1")
                .build();
            Tag updatedResourceTag2 = Tag.builder()
                    .key("resource-tag-key-2")
                    .value("resource-tag-updated-value-2")
                    .build();
            TagResourceRequest tagResourceRequest = TagResourceRequest.builder()
```

```
                    .resourceArn(resourceARN)
                    .tags(updatedResourceTag1, updatedResourceTag2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.tagResource(tagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Supprimer une balise de AWS ressource d'un groupe Storage Lens

Les exemples suivants montrent comment supprimer une balise de AWS ressource d'un groupe Storage Lens. Vous pouvez supprimer des balises à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour supprimer une balise de AWS ressource d'un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Groupes Storage Lens.
3. Sous Groupes Storage Lens, choisissez le groupe Storage Lens que vous souhaitez mettre à jour.
4. Sous Balises de ressources AWS , sélectionnez la paire clé-valeur que vous souhaitez supprimer.
5. Sélectionnez Delete (Supprimer). La boîte de dialogue Supprimer les balises de ressources AWS s'affiche.

> **Note**
>
> Si des balises sont utilisées pour contrôler l'accès, cette action peut affecter les ressources associées. Une fois que vous avez définitivement supprimé une balise, elle ne peut pas être restaurée.

6. Choisissez Supprimer pour supprimer définitivement la paire clé-valeur.

En utilisant le AWS CLI

La AWS CLI commande suivante supprime deux balises de AWS ressources d'un groupe Storage Lens existant : Pour utiliser cet exemple de commande, remplacez-les *user input placeholders* par vos propres informations.

```
aws s3control untag-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/Marketing-
Department \
--region us-east-1 --tag-keys k1 k2
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant supprime deux balises de AWS ressources du groupe Storage Lens Amazon Resource Name (ARN) que vous spécifiez dans le compte*111122223333*. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.UntagResourceRequest;

public class UntagResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
```

```
            String tagKey1 = "resource-tag-key-1";
            String tagKey2 = "resource-tag-key-2";
            UntagResourceRequest untagResourceRequest = UntagResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .tagKeys(tagKey1, tagKey2)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.untagResource(untagResourceRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Liste des balises du groupe Storage Lens

Les exemples suivants montrent comment répertorier les balises de AWS ressources associées à un groupe Storage Lens. Vous pouvez répertorier les balises à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour consulter la liste des balises et des valeurs des balises d'un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Groupes Storage Lens.
3. Sous Groupes Storage Lens, choisissez le groupe Storage Lens qui vous intéresse.
4. Faites défiler la page jusqu'à la section Balises de ressources AWS . Toutes les balises de AWS ressources définies par l'utilisateur qui sont ajoutées à votre groupe Storage Lens sont répertoriées avec leurs valeurs de balise.

En utilisant le AWS CLI

L' AWS CLI exemple de commande suivant répertorie toutes les valeurs des balises du groupe Storage Lens pour le groupe Storage Lens nommé*marketing-department*. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control list-tags-for-resource --account-id 111122223333 \
--resource-arn arn:aws:s3:us-east-1:111122223333:storage-lens-group/marketing-
department \
--region us-east-1
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant répertorie les valeurs des balises de groupe Storage Lens pour le groupe Storage Lens Amazon Resource Name (ARN) que vous spécifiez. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceRequest;
import software.amazon.awssdk.services.s3control.model.ListTagsForResourceResponse;

public class ListTagsForResource {
    public static void main(String[] args) {
        String resourceARN = "Resource_ARN";
        String accountId = "111122223333";

        try {
            ListTagsForResourceRequest listTagsForResourceRequest =
 ListTagsForResourceRequest.builder()
                    .resourceArn(resourceARN)
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
```

```
            ListTagsForResourceResponse response =
 s3ControlClient.listTagsForResource(listTagsForResourceRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Liste de tous les groupes Storage Lens

Les exemples suivants montrent comment répertorier tous les groupes Amazon S3 Storage Lens d'un Compte AWS et d'une région d'origine. Ces exemples montrent comment répertorier tous les groupes Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour répertorier tous les groupes Storage Lens d'un compte et d'une région d'origine

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Groupes Storage Lens.
3. Sous Groupes Storage Lens, la liste des groupes Storage Lens de votre compte s'affiche.

En utilisant le AWS CLI

L' AWS CLI exemple suivant répertorie tous les groupes Storage Lens de votre compte. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control list-storage-lens-groups --account-id 111122223333 \
--region us-east-1
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant répertorie les groupes Storage Lens pour le compte*111122223333*. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsRequest;
import software.amazon.awssdk.services.s3control.model.ListStorageLensGroupsResponse;

public class ListStorageLensGroups {
    public static void main(String[] args) {
        String accountId = "111122223333";

        try {
            ListStorageLensGroupsRequest listStorageLensGroupsRequest =
 ListStorageLensGroupsRequest.builder()
                    .accountId(accountId)
                    .build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            ListStorageLensGroupsResponse response =
 s3ControlClient.listStorageLensGroups(listStorageLensGroupsRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Affichage des détails d'un groupe Storage Lens

Les exemples suivants montrent comment afficher les détails de configuration d'un groupe Amazon S3 Storage Lens. Vous pouvez consulter ces informations à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour consulter les détails de configuration d'un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Groupes Storage Lens.
3. Sous Groupes Storage Lens, choisissez le bouton d'option en regard du groupe Storage Lens qui vous intéresse.
4. Sélectionnez Afficher les détails. Vous pouvez désormais passer en revue les détails de votre groupe Storage Lens.

En utilisant le AWS CLI

L' AWS CLI exemple suivant renvoie les détails de configuration d'un groupe Storage Lens. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant renvoie les détails de configuration du groupe Storage Lens nommé *Marketing-Department* dans le compte*111122223333*. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
```

```
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupRequest;
import software.amazon.awssdk.services.s3control.model.GetStorageLensGroupResponse;

public class GetStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            GetStorageLensGroupRequest getRequest =
 GetStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            GetStorageLensGroupResponse response =
 s3ControlClient.getStorageLensGroup(getRequest);
            System.out.println(response);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Suppression d'un groupe Storage Lens

Les exemples suivants montrent comment supprimer un groupe Amazon S3 Storage Lens à l'aide de la console Amazon S3, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java.

Utilisation de la console S3

Pour supprimer un groupe Storage Lens

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Groupes Storage Lens.
3. Sous Groupes Storage Lens, cliquez sur le bouton d'option en regard du groupe Storage Lens que vous souhaitez supprimer.
4. Sélectionnez Delete (Supprimer). La boîte de dialogue Supprimer le groupe Storage Lens s'affiche.
5. Choisissez à nouveau Supprimer pour supprimer définitivement votre groupe Storage Lens.

> **Note**
>
> Une fois que vous avez supprimé un groupe Storage Lens, il ne peut pas être restauré.

En utilisant le AWS CLI

L' AWS CLI exemple suivant supprime le groupe Storage Lens nommé*marketing-department*. Pour utiliser cet exemple de commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control delete-storage-lens-group --account-id 111122223333 \
--region us-east-1 --name marketing-department
```

Utilisation du AWS SDK pour Java

L' AWS SDK pour Java exemple suivant supprime le groupe Storage Lens nommé *Marketing-Department* dans le compte*111122223333*. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
package aws.example.s3control;

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.auth.credentials.ProfileCredentialsProvider;
```

```
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.DeleteStorageLensGroupRequest;

public class DeleteStorageLensGroup {
    public static void main(String[] args) {
        String storageLensGroupName = "Marketing-Department";
        String accountId = "111122223333";

        try {
            DeleteStorageLensGroupRequest deleteStorageLensGroupRequest =
 DeleteStorageLensGroupRequest.builder()
                    .name(storageLensGroupName)
                    .accountId(accountId).build();
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                    .region(Region.US_WEST_2)
                    .credentialsProvider(ProfileCredentialsProvider.create())
                    .build();
            s3ControlClient.deleteStorageLensGroup(deleteStorageLensGroupRequest);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it and returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }
}
```

Catalogage et analyse de vos données avec l'inventaire S3

Vous pouvez utiliser l'inventaire Amazon S3 pour vous aider à gérer votre stockage. Par exemple, vous pouvez l'utiliser pour contrôler et signaler le statut de réplication et de chiffrement de vos objets à des fins professionnelles, de conformité et d'obligations réglementaires. Vous pouvez également simplifier et accélérer les flux de travail et les tâches du big data à l'aide de l'inventaire Amazon S3, qui fournit une alternative planifiée aux opérations d'API `List` synchrones Amazon S3. L'inventaire Amazon S3 n'utilise pas les opérations d'API `List` pour auditer vos objets et n'affecte pas le taux de demande de votre compartiment.

L'inventaire Amazon S3 fournit des fichiers de sortie au format CSV (valeurs séparées par une virgule), ORC (Apache Optimized Row Columnar) ou Apache Parquet qui répertorient vos objets et leurs métadonnées correspondantes tous les jours ou toutes les semaines pour des objets ou un compartiment S3 avec un préfixe partagé (c'est-à-dire des objets dont le nom commence par une chaîne commune). Si vous avez configuré un inventaire hebdomadaire, un rapport est généré tous les dimanches (fuseau horaire UTC) après le rapport initial. Pour plus d'informations sur la tarification de l'inventaire Amazon S3, consultez Tarification Amazon S3.

Vous pouvez configurer plusieurs listes d'inventaire d'un compartiment. Lorsque vous configurez une liste d'inventaire, vous pouvez spécifier les éléments suivants :

- Quelles métadonnées d'objet inclure dans l'inventaire
- S'il faut répertorier toutes les versions de l'objet ou uniquement les versions actuelles
- Où stocker la sortie du fichier de liste d'inventaire
- S'il faut générer l'inventaire de manière quotidienne ou hebdomadaire
- S'il faut chiffrer le fichier de liste d'inventaire

Vous pouvez interroger l'inventaire Amazon S3 avec des requêtes SQL standard en utilisant Amazon Athena, Amazon Redshift Spectrum et d'autres outils tels que Presto, Apache Hive et Apache Spark. Pour plus d'informations sur l'utilisation d'Athena pour interroger vos fichiers d'inventaire, consultez the section called "Interrogation d'un inventaire avec Athena".

> **Note**
>
> La distribution du premier rapport d'inventaire pour Amazon S3 peut prendre jusqu'à 48 heures.

Compartiments source et de destination

Le compartiment pour lequel l'inventaire répertorie les objets est appelé compartiment source. Le compartiment dans lequel le fichier de liste d'inventaire est stocké est appelé compartiment de destination.

Compartiment source

L'inventaire répertorie les objets qui sont stockés dans le compartiment source. Vous pouvez obtenir une liste d'inventaire d'un compartiment entier ou vous pouvez filtrer par liste par préfixe de nom de la clé d'objet.

Le compartiment source :

- Contient les objets qui sont répertoriés dans l'inventaire
- Contient la configuration de l'inventaire

Compartiment de destination

Les fichiers de liste d'inventaire Amazon S3 sont écrits dans le compartiment de destination. Vous pouvez spécifier un préfixe de destination dans la configuration de l'inventaire pour regrouper tous les fichiers de liste d'inventaire dans un emplacement commun au sein du compartiment de destination.

Le compartiment de destination :

- Contient les listes de fichiers d'inventaire.
- Contient les fichiers manifeste qui répertorient tous les fichiers de listes d'inventaire stockés dans le compartiment de destination. Pour plus d'informations, consultez Manifeste d'inventaire.
- Doit avoir une politique de compartiment pour donner à Amazon S3 l'autorisation de vérifier la propriété du compartiment et l'autorisation d'écrire des fichiers dans le compartiment.
- Doit se trouver dans le même compartiment Région AWS que le compartiment source.
- Peut être le même que le compartiment source.
- Peut appartenir à un compte Compte AWS différent du compte propriétaire du bucket source.

Liste d'inventaire Amazon S3

Un fichier de liste d'inventaire contient une liste des objets figurant dans le compartiment source et les métadonnées de chaque objet. Un fichier de liste d'inventaire est stocké dans le compartiment de destination sous l'un des formats suivants :

- Fichier CSV compressé avec GZIP
- En tant que fichier de colonne de ligne optimisée (ORC) par Apache compressé avec ZLIB
- En tant que fichier Apache Parquet compressé avec Snappy

> **Note**
>
> Le tri des objets n'est pas garanti dans les rapports d'inventaire Amazon S3.

Un fichier de liste d'inventaire contient une liste des objets figurant dans le compartiment source et les métadonnées de chaque objet figurant dans la liste :

- Nom du compartiment – Le nom du compartiment pour lequel l'inventaire est effectué.
- Nom de clé – Nom de la clé d'objet (ou clé) qui identifie de manière unique l'objet dans le compartiment. Lorsque vous utilisez le format de fichier CSV, le nom de clé est codé en URL et doit être décodé avant d'être utilisé.
- ID de version – ID de version de l'objet. Lorsque vous activez la gestion des versions sur un compartiment, Amazon S3 attribue un numéro de version aux objets qui sont ajoutés au compartiment. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3. (Ce champ n'est pas inclus si la liste est configurée uniquement pour la version actuelle des objets.)
- IsLatest— Défini sur `True` si l'objet est la version actuelle de l'objet. (Ce champ n'est pas inclus si la liste est configurée uniquement pour la version actuelle des objets.)
- Marqueur de suppression – Défini sur `True`, si l'objet est un marqueur de suppression. Pour plus d'informations, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3. (Ce champ est automatiquement ajouté à votre rapport si vous avez configuré celui-ci pour qu'il inclue toutes les versions de vos objets).
- Taille : la taille de l'objet en octets, à l'exclusion de la taille des chargements partitionnés incomplets, des métadonnées de l'objet et des marqueurs de suppression.
- Date de la dernière modification – Date de création de l'objet ou date de la dernière modification, la plus récente étant retenue.
- ETag— La balise d'entité (ETag) est un hachage de l'objet. Le ETag reflète les modifications apportées uniquement au contenu d'un objet, et non à ses métadonnées. Il ETag peut s'agir d'un MD5 condensé des données de l'objet. Cela dépend de la façon dont l'objet a été créé et de la manière dont il est chiffré. Pour plus d'informations, consultez Object dans la Référence d'API Amazon Simple Storage Service.
- Classe de stockage : classe de stockage utilisée pour stocker l'objet. Défini sur `STANDARD`, `REDUCED_REDUNDANCY`, `STANDARD_IA`, `ONEZONE_IA`, `INTELLIGENT_TIERING`, `GLACIER`,

`DEEP_ARCHIVE`, `OUTPOSTS`, `GLACIER_IR` ou `SNOW`. Pour de plus amples informations, veuillez consulter Bien comprendre et gérer les classes de stockage Amazon S3.

> **Note**
>
> L'inventaire S3 ne prend pas en charge S3 Express One Zone.

- Indicateur de chargement partitionné – Défini sur `True` si l'objet a été chargé dans un chargement partitionné. Pour plus d'informations, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.
- Statut de réplication – Défini sur `PENDING`, `COMPLETED`, `FAILED` ou `REPLICA`. Pour de plus amples informations, veuillez consulter Obtention d'informations sur le statut de la réplication.
- État du chiffrement — État du chiffrement côté serveur, en fonction du type de clé de chiffrement utilisé : chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3), chiffrement côté serveur avec des clés () (SSE-KMS), chiffrement côté serveur double couche avec clés AWS Key Management Service (AWS KMS DSSE-KMS) ou chiffrement côté serveur avec des AWS KMS clés fournies par le client (SSE-C). Défini sur `SSE-S3`, `SSE-KMS`, `DSSE-KMS`, `SSE-C` ou `NOT-SSE`. Le statut `NOT-SSE` signifie que l'objet n'est pas chiffré avec le chiffrement côté serveur. Pour plus d'informations, consultez Protection des données à l'aide du chiffrement.
- Date de fin de conservation du verrouillage d'objet S3 : date jusqu'à laquelle l'objet verrouillé ne peut pas être supprimé. Pour plus d'informations, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.
- Mode de rétention de verrouillage d'objet S3 : défini sur `Governance` ou `Compliance` pour les objets qui sont verrouillés. Pour plus d'informations, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.
- Statut de conservation légale du verrouillage d'objet S3 : défini sur 0n si une conservation légale a été appliquée à un objet. Sinon, elle est définie sur `Off`. Pour plus d'informations, consultez Verrouillage d'objets avec la fonctionnalité de verrouillage d'objet.
- Niveau d'accès S3 Intelligent-Tiering : niveau d'accès (fréquent ou peu fréquent) de l'objet s'il est stocké dans S3 Intelligent-Tiering. Définissez sur `FREQUENT`, `INFREQUENT`, `ARCHIVE_INSTANT_ACCESS`, `ARCHIVE` ou `DEEP_ARCHIVE`. Pour plus d'informations, consultez Classe de stockage pour l'optimisation automatique des données avec des modèles d'accès inconnus ou irréguliers.

- Statut de clé de compartiment S3 – Défini sur `ENABLED` ou `DISABLED`. Indique si l'objet utilise une clé de compartiment S3 pour SSE-KMS. Pour plus d'informations, consultez Utilisation de clés de compartiment Amazon S3..
- Algorithme de total de contrôle : algorithme utilisé pour créer le total de contrôle de l'objet. Pour de plus amples informations, veuillez consulter Utilisation des algorithmes de total de contrôle pris en charge.
- Liste de contrôle d'accès aux objets : liste de contrôle d'accès (ACL) pour chaque objet qui définit le Comptes AWS ou les groupes autorisés à accéder à cet objet et le type d'accès accordé. Le champ Liste ACL d'objet est défini au format JSON. Un rapport d'inventaire S3 inclut ACLs les objets associés aux objets de votre compartiment source, même lorsqu'ils ACLs sont désactivés pour le compartiment. Pour plus d'informations, consultez Utiliser le champ Liste ACL d'objet et Présentation de la liste de contrôle d'accès (ACL).

> **Note**
>
> Le champ Liste ACL d'objet est défini au format JSON. Un rapport d'inventaire affiche la valeur du champ Liste ACL d'objet sous la forme d'une chaîne codée en base64. Supposons, par exemple, que vous disposiez du champ Liste ACL d'objet suivant au format JSON :
>
> ```
> {
>         "version": "2022-11-10",
>         "status": "AVAILABLE",
>         "grants": [{
>             "canonicalId": "example-canonical-user-ID",
>             "type": "CanonicalUser",
>             "permission": "READ"
>         }]
> }
> ```
>
> Le champ Liste ACL d'objet est codé et affiché sous la forme de la chaîne codée en base64 suivante :
>
> ```
> eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2Fs
> ```

Pour obtenir la valeur décodée au format JSON pour le champ Liste ACL d'objet, vous pouvez interroger ce champ dans Amazon Athena. Pour d'autres exemples de requête, consultez Interrogation d'un inventaire Amazon S3 avec Amazon Athena.

- Propriétaire de l'objet – ID d'utilisateur canonique du propriétaire de l'objet. Pour plus d'informations, voir Trouver l'ID utilisateur canonique de votre AWS compte dans le Guide de référence sur la gestion des AWS comptes.

> **Note**
>
> Lorsqu'un objet est en fin de vie selon la configuration de son cycle de vie, Amazon S3 le place dans une file d'attente en vue de sa suppression et le supprime de manière asynchrone. Cependant, un certain retard est possible entre la date d'expiration et la date à laquelle Amazon S3 supprime l'objet. Le rapport d'inventaire inclut les objets qui ont expiré mais qui n'ont pas encore été supprimés. Pour plus d'informations sur les actions d'expiration dans le cycle de vie S3, consultez Objets en cours d'expiration.

Voici un exemple de rapport d'inventaire avec des champs de métadonnées supplémentaires, qui se compose de quatre enregistrements.

```
amzn-s3-demo-bucket1    example-object-1    EXAMPLEDC8l.XJCENlF7LePaNIIvs001    TRUE
     1500    2024-08-15T15:28:26.0004    EXAMPLE21e1518b92f3d92773570f600    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7000
amzn-s3-demo-bucket1    example-object-2    EXAMPLEDC8l.XJCENlF7LePaNIIvs002
 TRUE        200    2024-08-21T15:28:26.000Z    EXAMPLE21e1518b92f3d92773570f601
  INTELLIGENT_TIERING    FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z
    COMPLIANCE    Off    INFREQUENT    ENABLED    SHA-256
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7001
amzn-s3-demo-bucket1    example-object-3    EXAMPLEDC8l.XJCENlF7LePaNIIvs003    TRUE
      12500    2023-01-15T15:28:30.000Z    EXAMPLE21e1518b92f3d92773570f602    STANDARD
    FALSE    REPLICA    SSE-KMS    2025-01-25T15:28:26.000Z    GOVERNANCE    On
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7002
```

```
amzn-s3-demo-bucket1    example-object-4    EXAMPLEDC8l.XJCENlF7LePaNIIvs004    TRUE
      100    2021-02-15T15:28:27.000Z    EXAMPLE21e1518b92f3d92773570f603    STANDARD
  FALSE    COMPLETED    SSE-KMS    2025-01-25T15:28:26.000Z    COMPLIANCE    Off
 ENABLED
 eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3sicGVybWlzc2lvbiI6Ik
    EXAMPLE766e8f6b115d93d41df2eac420aa4a465d177c1398bc6a088c76b7003
```

Nous vous recommandons de créer une stratégie de cycle de vie qui supprime les anciennes listes d'inventaire. Pour plus d'informations, consultez Gestion du cycle de vie des objets.

L'autorisation `s3:PutInventoryConfiguration` permet à l'utilisateur de sélectionner tous les champs de métadonnées répertoriés précédemment pour chaque objet lors de la configuration d'une liste d'inventaire et de spécifier le compartiment de destination pour stocker l'inventaire. Un utilisateur disposant d'un accès en lecture aux objets du compartiment de destination peut accéder à tous les champs de métadonnées d'objets disponibles dans la liste d'inventaire. Pour restreindre l'accès à un rapport d'inventaire, consultez Accorder des autorisations pour l'inventaire S3 et les analyses S3..

Cohérence de l'inventaire

Tous vos objets peuvent ne pas apparaître dans chaque liste d'inventaire. La liste d'inventaire fournit une cohérence à terme pour des requêtes PUT (des objets nouveaux et de remplacement) et pour des requêtes `DELETE`. Chaque liste d'inventaire d'un compartiment est un instantané des articles du compartiment. Ces listes sont finalement cohérentes (c'est-à-dire qu'une liste peut ne pas inclure les objets récemment ajoutés ou supprimés).

Pour valider l'état d'un objet avant de prendre des mesures sur l'objet, nous recommandons d'effectuer une demande d'API REST `HeadObject` pour récupérer les métadonnées de l'objet ou de vérifier les propriétés de l'objet dans la console Amazon S3. Vous pouvez également vérifier les métadonnées des objets avec le AWS CLI ou les AWS SDK. Pour plus d'informations, veuillez consulter `HeadObject` dans la Référence d'API Amazon Simple Storage Service.

Pour plus d'informations sur l'utilisation de l'inventaire Amazon S3, consultez les rubriques suivantes.

Rubriques

- Configuration de l'inventaire Amazon S3
- Localisation de votre liste d'inventaire
- Configuration des notifications d'événements Amazon S3 pour l'achèvement de l'inventaire
- Interrogation d'un inventaire Amazon S3 avec Amazon Athena

- Conversion de chaînes d'ID de version vides dans les rapports d'inventaire Amazon S3 en chaînes null
- Utiliser le champ Liste ACL d'objet

Configuration de l'inventaire Amazon S3

L'inventaire Amazon S3 fournit une liste de fichiers plats de vos objets et métadonnées, selon un calendrier que vous définissez. Vous pouvez utiliser S3 Inventory comme une autre solution planifiée de l'opération d'API `List` synchrone d'Amazon S3. S3 Inventory fournit des fichiers de sortie au format CSV (valeurs séparées par une virgule), ORC (Apache Optimized Row Columnar) ou Apache Parquet (Parquet) qui répertorient vos objets et leurs métadonnées correspondantes.

Vous pouvez configurer S3 Inventory afin de créer des listes d'inventaire de façon quotidienne ou hebdomadaire pour un compartiment S3 ou pour des objets qui partagent un préfixe (c'est-à-dire des objets dont le nom commence avec la même chaîne). Pour de plus amples informations, veuillez consulter Catalogage et analyse de vos données avec l'inventaire S3.

Cette section explique comment configurer un inventaire, avec notamment des détails sur les compartiments source et de destination.

Rubriques

- Présentation
- Création d'une politique de compartiment de destination
- Octroi à Amazon S3 d'utiliser votre clé gérée par le client pour le chiffrement
- Configuration de l'inventaire à l'aide de la console S3
- Utilisation de l'API REST pour travailler avec l'inventaire S3

Présentation

Amazon S3 Inventory vous aide à gérer votre stockage en créant des listes d'objets dans un compartiment S3 selon une planification définie. Vous pouvez configurer plusieurs listes d'inventaire d'un compartiment. Les listes d'inventaire sont publiées dans des fichiers CSV, ORC, ou Parquet au sein d'un compartiment de destination.

Le moyen le plus simple de configurer un inventaire est d'utiliser la console Amazon S3, mais vous pouvez également utiliser l'API REST Amazon S3, AWS Command Line Interface (AWS CLI) ou

AWS SDKs. La console effectue la première étape de la procédure suivante pour vous : ajouter une politique de compartiment au compartiment de destination.

Pour configure Amazon S3 Inventory pour un compartiment S3

1. Ajoutez une politique de compartiment pour le compartiment de destination.

   Vous devez créer une politique de compartiment au niveau du compartiment de destination pour accorder à Amazon S3 l'autorisation d'écrire des objets dans le compartiment à l'emplacement défini. Pour un exemple de politique, consultez Accorder des autorisations pour l'inventaire S3 et les analyses S3..
2. Configurez un inventaire pour répertorier les objets dans un compartiment source et publier la liste dans un compartiment de destination.

   Lorsque vous configurez une liste d'inventaire pour un compartiment source, vous spécifiez le compartiment de destination dans lequel vous voulez stocker la liste et la fréquence de génération de la liste (quotidienne ou hebdomadaire). Vous pouvez également choisir de répertorier toutes les versions d'objet ou uniquement les versions actuelles, ainsi que les métadonnées à inclure.

   Certains champs de métadonnées d'objet dans les configurations des rapports d'inventaire S3 sont facultatifs. En d'autres termes, ils sont disponibles par défaut, mais ils peuvent être restreints lorsque vous accordez l'autorisation `s3:PutInventoryConfiguration` à un utilisateur. Vous pouvez contrôler si les utilisateurs peuvent inclure ces champs de métadonnées facultatifs dans leurs rapports à l'aide de la clé de condition `s3:InventoryAccessibleOptionalFields`.

   Pour plus d'informations sur les champs de métadonnées facultatifs disponibles dans l'inventaire S3, consultez OptionalFields dans la Référence d'API Amazon Simple Storage Service. Pour plus d'informations sur la restriction de l'accès à certains champs de métadonnées facultatifs dans une configuration d'inventaire, consultez Création de la configuration des rapports d'inventaire S3.

   Vous pouvez spécifier que le fichier de liste d'inventaire doit être chiffré en utilisant le chiffrement côté serveur avec une clé gérée Amazon S3 (SSE-S3) ou une clé gérée par le client AWS Key Management Service (SSE-KMS AWS KMS).

   > **Note**
   >
   > Le Clé gérée par AWS (`aws/s3`) n'est pas pris en charge pour le chiffrement SSE-KMS avec S3 Inventory.

Pour en savoir plus sur SSE-S3 et SSE-KMS, consultez Protection des données avec le chiffrement côté serveur. Si vous prévoyez d'utiliser le chiffrement SSE-KMS, consultez l'étape 3.

- Pour plus d'informations sur l'utilisation de la console pour configurer une liste d'inventaire, consultez Configuration de l'inventaire à l'aide de la console S3.
- Pour utiliser l'API Amazon S3 afin de configurer une liste d'inventaire, utilisez l'opération d'PutBucketInventoryConfigurationAPI REST ou l'équivalent du AWS CLI ou AWS SDKs.

3. Pour chiffrer le fichier de liste d'inventaire avec SSE-KMS, autorisez Amazon S3 à utiliser la AWS KMS key.

   Vous pouvez configurer le chiffrement du fichier de liste d'inventaire à l'aide de la console Amazon S3, de l'API REST Amazon S3 ou AWS SDKs. AWS CLI Quelle que soit la méthode que vous choisissez, vous devez autoriser Amazon S3 à utiliser la clé gérée par le client pour chiffrer le fichier d'inventaire. Vous accordez l'autorisation à Amazon S3 en modifiant la politique relative aux clés gérées par le client que vous souhaitez utiliser pour chiffrer le fichier d'inventaire. Assurez-vous d'avoir fourni un ARN de clé KMS dans la configuration de l'inventaire S3 ou dans les paramètres de chiffrement du compartiment de destination. Si aucun ARN de clé KMS n'a été spécifié et que les paramètres de chiffrement par défaut sont utilisés, vous ne pourrez pas accéder à votre rapport d'inventaire S3.

   Le compartiment de destination qui stocke le fichier de liste d'inventaire peut appartenir à un autre Compte AWS que le compte propriétaire du compartiment source. Si vous utilisez le chiffrement SSE-KMS pour les opérations intercomptes de l'inventaire Amazon S3, lorsque vous configurez l'inventaire S3, nous vous recommandons d'utiliser un ARN de clé KMS complet. Pour plus d'informations, consultez Utilisation du chiffrement SSE-KMS pour les opérations intercomptes et ServerSideEncryptionByDefault dans la référence de l'API Amazon Simple Storage Service.

   > **Note**
   >
   > Si vous ne pouvez pas accéder à votre rapport d'inventaire S3, vérifiez si le chiffrement SSE-KMS par défaut est activé dans le compartiment de destination. Si aucun ARN de clé KMS n'a été spécifié et que les paramètres de chiffrement par défaut sont utilisés, vous ne pourrez pas accéder à votre rapport d'inventaire S3. Pour accéder à votre rapport d'inventaire, fournissez un ARN de clé KMS dans la configuration de l'inventaire S3 ou dans les paramètres de chiffrement du compartiment de destination.

Création d'une politique de compartiment de destination

Si vous créez votre configuration d'inventaire via la console Amazon S3, Amazon S3 crée automatiquement une politique de compartiment sur le compartiment de destination qui accorde une autorisation d'écriture Amazon S3 au compartiment. Toutefois, si vous créez votre configuration d'inventaire par le biais de AWS CLI AWS SDKs, ou de l'API REST Amazon S3, vous devez ajouter manuellement une politique de compartiment sur le compartiment de destination. La politique de compartiment de destination de l'inventaire Amazon S3 autorise Amazon S3 à écrire des données pour les rapports d'inventaire dans ce compartiment.

Voici un exemple de politique de compartiment.

JSON

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
            "Sid": "InventoryExamplePolicy",
            "Effect": "Allow",
            "Principal": {
                "Service": "s3.amazonaws.com"
            },
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::DOC-EXAMPLE-DESTINATION-BUCKET/*"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:SourceArn": "arn:aws:s3:::DOC-EXAMPLE-SOURCE-BUCKET"
                },
                "StringEquals": {
                    "aws:SourceAccount": "source-account-id",
                    "s3:x-amz-acl": "bucket-owner-full-control"
                }
            }
        }
    ]
}
```

Pour de plus amples informations, veuillez consulter Accorder des autorisations pour l'inventaire S3 et les analyses S3..

Si une erreur se produit lorsque vous tentez de créer la politique de compartiment, des instructions s'affichent pour vous indiquer comment la résoudre. Par exemple, si vous choisissez un compartiment de destination dans un autre Compte AWS et que vous n'êtes pas autorisé à lire et à écrire dans la politique du compartiment, un message d'erreur s'affiche.

Dans ce cas, le propriétaire du compartiment de destination doit ajouter la politique de compartiment affichée au compartiment de destination. Si la politique n'est pas ajoutée au compartiment de destination, vous ne recevez pas de rapport d'inventaire, car Amazon S3 n'est pas autorisé à écrire dans le compartiment de destination. Si le compartiment source est détenu par un compte autre que celui de l'utilisateur actuel, l'ID de compte correct du propriétaire du compartiment source doit être remplacé dans la politique.

> **Note**
>
> Assurez-vous qu'aucune instruction Deny n'est ajoutée à la politique du compartiment de destination. Cela empêcherait la livraison des rapports d'inventaire dans ce compartiment. Pour plus d'informations, consultez Pourquoi ne puis-je pas générer un rapport d'inventaire Amazon S3 ?.

Octroi à Amazon S3 d'utiliser votre clé gérée par le client pour le chiffrement

Pour autoriser Amazon S3 à utiliser votre clé gérée par le client AWS Key Management Service (AWS KMS) pour le chiffrement côté serveur, vous devez utiliser une politique de clé. Pour mettre à jour votre stratégie de clé et pouvoir utiliser votre clé gérée par le client, suivez la procédure suivante.

Pour accorder les autorisations Amazon S3 pour le chiffrement à l'aide de votre clé gérée par le client

1. À l'aide du Compte AWS propriétaire de la clé gérée par le client, connectez-vous au AWS Management Console.
2. Ouvrez la AWS KMS console à l'adresse https://console.aws.amazon.com/kms.
3. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page.
4. Dans le panneau de navigation de gauche, choisissez Clés gérées par le client.

5. Sous Clés gérées par le client, choisissez la clé gérée par le client que vous souhaitez utiliser pour chiffrer vos fichiers d'inventaire.
6. Dans la section Key policy (Politique de clé), sélectionnez Switch to policy view (Passer à la vue de politique).
7. Pour mettre à jour la politique de clé, choisissez Modifier.
8. Sous Modifier la stratégie de clé, ajoutez les lignes suivantes à la stratégie de clé existante. Pour *source-account-id* et *amzn-s3-demo-source-bucket*, fournissez les valeurs appropriées pour votre cas d'utilisation.

```
{
    "Sid": "Allow Amazon S3 use of the customer managed key",
    "Effect": "Allow",
    "Principal": {
        "Service": "s3.amazonaws.com"
    },
    "Action": [
        "kms:GenerateDataKey"
    ],
    "Resource": "*",
    "Condition":{
      "StringEquals":{
         "aws:SourceAccount":"source-account-id"
     },
      "ArnLike":{
        "aws:SourceARN": "arn:aws:s3:::amzn-s3-demo-source-bucket"
     }
   }
}
```

9. Sélectionnez Enregistrer les modifications.

Pour en savoir plus amples sur la création de clés gérées par le client et l'utilisation de politiques de clé, cliquez sur les liens suivants dans le guide du développeur AWS Key Management Service :

- Gestion des clés
- Politiques clés en AWS KMS

> **Note**
>
> Assurez-vous qu'aucune instruction Deny n'est ajoutée à la politique du compartiment de destination. Cela empêcherait la livraison des rapports d'inventaire dans ce compartiment. Pour plus d'informations, consultez Pourquoi ne puis-je pas générer un rapport d'inventaire Amazon S3 ?.

Configuration de l'inventaire à l'aide de la console S3

Suivez ces instructions pour configurer l'inventaire à l'aide de la console S3.

> **Note**
>
> La distribution du premier rapport d'inventaire pour Amazon S3 peut prendre jusqu'à 48 heures.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez configurer Amazon S3 Inventory.
4. Choisissez l'onglet Gestion.
5. Sous Configurations d'inventaire, choisissez Créer une configuration d'inventaire.
6. Dans Nom de la configuration d'inventaire, saisissez un nom.
7. Pour Portée de l'inventaire, procédez comme suit :
   - Entrez un préfixe facultatif.
   - Choisissez les versions d'objet à inclure, soit Versions actuelles uniquement, soit Inclure toutes les versions.
8. Sous Report details (Détails du rapport), choisissez l'emplacement du Compte AWS où vous souhaitez enregistrer les rapports : This account (Ce compte) ou A different account (Un compte différent).
9. Sous Destination, choisissez le compartiment de destination dans lequel vous souhaitez que les rapports d'inventaire soient enregistrés.

Le compartiment de destination doit se trouver dans le même compartiment Région AWS que celui pour lequel vous configurez l'inventaire. Le compartiment de destination peut se trouver dans un autre Compte AWS. Lorsque vous spécifiez le compartiment de destination, vous pouvez également inclure un préfixe facultatif pour regrouper vos rapports d'inventaire.

Sous le champ de compartiment Destination vous voyez la déclaration Autorisation de compartiment de destination qui est ajoutée à la politique de compartiment de destination pour permettre à Amazon S3 de placer des données dans ce compartiment. Pour de plus amples informations, veuillez consulter Création d'une politique de compartiment de destination.

10. Sous Fréquence, choisissez la fréquence à laquelle le rapport sera généré : Quotidien ou Hebdomadaire.
11. Dans Format de sortie, choisissez l'un des formats suivants pour le rapport :

    - CSV : si vous prévoyez d'utiliser ce rapport d'inventaire avec S3 Batch Operations ou si vous souhaitez analyser ce rapport dans un autre outil, tel que Microsoft Excel, choisissez CSV.
    - Apache ORC
    - Apache Parquet
12. Sous Status (Statut), choisissez Enable (Activer) ou Disable (Désactiver).
13. Pour configurer le chiffrement côté serveur, sous Chiffrement des rapports d'inventaire, procédez comme suit :

    a. Sous Chiffrement côté serveur, choisissez Ne pas spécifier de clé de chiffrement ou Spécifier une clé de chiffrement pour chiffrer les données.

    - Pour conserver les paramètres du compartiment pour le chiffrement côté serveur par défaut des objets lors de leur stockage dans Amazon S3, choisissez Ne pas spécifier de clé de chiffrement. Tant que les clés de compartiment S3 sont activées pour la destination du compartiment, l'opération de copie applique une clé de compartiment S3 au compartiment de destination.

      > **Note**
      >
      > Si la politique de compartiment pour la destination spécifiée exige que les objets soient chiffrés avant de les stocker dans Amazon S3, vous devez choisir Spécifier une clé de chiffrement. Sinon, la copie des objets vers la destination échouera.

- Pour chiffrer des objets avant de les stocker dans Amazon S3, choisissez Spécifier une clé de chiffrement.

b. Si vous avez choisi Spécifier une clé de chiffrement, sous Type de chiffrement, vous devez choisir Clé gérée par Amazon S3 (SSE-S3) ou CléAWS Key Management Service (SSE-KMS).

SSE-S3 utilise l'un des chiffrements par bloc les plus puissants qui existent, Advanced Encryption Standard à 256 bits (AES-256) pour chiffrer chaque objet. SSE-KMS vous permet de mieux contrôler votre clé. Pour en savoir plus sur SSE-S3, consultez Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3). Pour en savoir plus sur SSE-KMS, consultez Utilisation du chiffrement côté serveur à l'aide de AWS KMS clés (SSE-KMS).

> **Note**
>
> Pour chiffrer le fichier de liste d'inventaire avec SSE-KMS, vous devez autoriser Amazon S3 à utiliser la clé gérée par le client. Pour obtenir des instructions, consultez Octroyer à Amazon S3 l'autorisation d'utiliser vos clés KMS pour le chiffrement.

c. Si vous avez choisi AWS Key Management Service clé (SSE-KMS), sous AWS KMS key, vous pouvez spécifier votre AWS KMS clé à l'aide de l'une des options suivantes.

> **Note**
>
> Si le compartiment de destination qui stocke le fichier de liste d'inventaire appartient à un autre Compte AWS utilisateur, assurez-vous d'utiliser un ARN de clé KMS complet pour spécifier votre clé KMS.

- Pour choisir parmi une liste de clés KMS disponibles, choisissez Choisir parmi vos AWS KMS clés, puis choisissez une clé KMS de chiffrement symétrique dans la liste des clés disponibles. Vérifiez que la clé KMS se situe dans la même région que votre compartiment.

> **Note**
>
> La clé Clé gérée par AWS (`aws/s3`) et la clé gérée par votre client apparaissent toutes deux dans la liste. Cependant, le Clé gérée par AWS (`aws/s3`) n'est pas pris en charge pour le chiffrement SSE-KMS avec S3 Inventory.

- Pour saisir l'ARN de la clé KMS, choisissez Enter AWS KMS key ARN, puis saisissez l'ARN de votre clé KMS dans le champ qui apparaît.
- Pour créer une nouvelle clé gérée par le client dans la AWS KMS console, choisissez Create a KMS key.

14. Pour Champs de métadonnées supplémentaires, sélectionnez un ou plusieurs des éléments suivants à ajouter au rapport d'inventaire :

    - Taille : la taille de l'objet en octets, à l'exclusion de la taille des chargements partitionnés incomplets, des métadonnées de l'objet et des marqueurs de suppression.
    - Date de la dernière modification – Date de création de l'objet ou date de la dernière modification, la plus récente étant retenue.
    - Multipart upload (Chargement partitionné) – Spécifie que l'objet a été chargé dans un chargement partitionné. Pour de plus amples informations, veuillez consulter Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.
    - Replication status (Statut de réplication) – Statut de réplication de l'objet. Pour de plus amples informations, veuillez consulter Obtention d'informations sur le statut de la réplication.
    - Statut de chiffrement : chiffrement côté serveur utilisé pour chiffrer l'objet. Pour de plus amples informations, veuillez consulter Protection des données avec le chiffrement côté serveur.
    - État de la clé du compartiment : indique si une clé au niveau du compartiment générée par AWS KMS s'applique à l'objet. Pour de plus amples informations, veuillez consulter Réduction du coût du SSE-KMS avec les clés de compartiment Amazon S3.
    - Liste de contrôle d'accès aux objets : liste de contrôle d'accès (ACL) pour chaque objet qui définit le Comptes AWS ou les groupes autorisés à accéder à cet objet et le type d'accès accordé. Pour plus d'informations sur ce champ, consultez Utiliser le champ Liste ACL d'objet. Pour plus d'informations sur ACLs, voirPrésentation de la liste de contrôle d'accès (ACL).
    - Propriétaire de l'objet : le propriétaire de l'objet.
    - Classe de stockage : classe de stockage utilisée pour stocker l'objet.

- Niveau d'accès Intelligent-Tiering : niveau d'accès (fréquent ou peu fréquent) de l'objet si celui-ci est stocké dans la classe de stockage S3 Intelligent-Tiering. Pour de plus amples informations, veuillez consulter Classe de stockage pour l'optimisation automatique des données avec des modèles d'accès inconnus ou irréguliers.
- ETag— La balise d'entité (ETag) est un hachage de l'objet. Le ETag reflète les modifications apportées uniquement au contenu d'un objet, et non à ses métadonnées. ETag Il peut s'agir ou non d'un MD5 résumé des données de l'objet. Cela dépend de la façon dont l'objet a été créé et de la manière dont il est chiffré. Pour plus d'informations, consultez Object dans la Référence d'API Amazon Simple Storage Service.
- Algorithme de total de contrôle : algorithme utilisé pour créer le total de contrôle de l'objet. Pour de plus amples informations, veuillez consulter Utilisation des algorithmes de total de contrôle pris en charge.
- Configurations du verrouillage de tous les objets : statut du verrouillage des objets, y compris les paramètres suivants :
  - Verrouillage d'objet : mode de rétention : niveau de protection appliqué à l'objet, Gouvernance ou Conformité.
  - Verrouillage d'objet : conserver jusqu'à la date : date jusqu'à laquelle l'objet verrouillé ne peut pas être supprimé.
  - Verrouillage d'objet : statut de la conservation légale : statut de la conservation légale de l'objet verrouillé.

  Pour de plus amples informations sur la fonctionnalité de verrouillage des objets S3, consultez Fonctionnement du verrouillage d'objets S3.

Pour plus d'informations sur le contenu d'un rapport d'inventaire, consultez Liste d'inventaire Amazon S3.

Pour plus d'informations sur la restriction de l'accès à certains champs de métadonnées facultatifs dans une configuration d'inventaire, consultez Création de la configuration des rapports d'inventaire S3.

15. Choisissez Créer.

Utilisation de l'API REST pour travailler avec l'inventaire S3

Les opérations REST utilisées pour travailler avec l'inventaire Amazon S3 sont les suivantes.

- DeleteBucketInventoryConfiguration
- GetBucketInventoryConfiguration
- ListBucketInventoryConfigurations
- PutBucketInventoryConfiguration

Localisation de votre liste d'inventaire

Lorsqu'une liste d'inventaire est publiée, les fichiers manifestes sont publiés dans l'emplacement suivant dans le compartiment de destination.

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/manifest.json
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/YYYY-MM-DDTHH-MMZ/
manifest.checksum
 destination-prefix/amzn-s3-demo-source-bucket/config-ID/hive/dt=YYYY-MM-DD-HH-MM/
symlink.txt
```

- *destination-prefix* est le préfixe de nom de la clé d'objet défini de manière facultative dans la configuration de l'inventaire. Vous pouvez utiliser ce préfixe pour regrouper tous les fichiers de liste d'inventaire dans un emplacement commun au sein du compartiment de destination.
- *amzn-s3-demo-source-bucket* est le compartiment source pour lequel la liste d'inventaire est effectuée. Le nom du compartiment source est ajouté pour éviter les collisions lorsque plusieurs rapports d'inventaire de différents compartiments source sont envoyés dans le même compartiment de destination.
- *config-ID* est ajouté pour éviter les collisions avec plusieurs rapports d'inventaire du même compartiment source qui sont envoyés dans le même compartiment de destination. Le *config-ID* provient de la configuration de rapport d'inventaire et est le nom du rapport défini lors de la configuration.
- *YYYY-MM-DDTHH-MMZ* est l'horodatage composé de l'heure de début et de la date à laquelle la génération de rapport d'inventaire a commencé à analyser le compartiment, par exemple, `2016-11-06T21-32Z`.
- `manifest.json` est le fichier manifeste.
- `manifest.checksum`est le MD5 hachage du contenu du `manifest.json` fichier.
- `symlink.txt` est le fichier manifeste compatible avec Apache Hive.

Les listes d'inventaire sont publiées sur une base quotidienne ou hebdomadaire dans l'emplacement suivant dans le compartiment de destination.

```
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name.csv.gz
...
destination-prefix/amzn-s3-demo-source-bucket/config-ID/data/example-file-name-1.csv.gz
```

- *destination-prefix* est le préfixe de nom de la clé d'objet défini de manière facultative dans la configuration de l'inventaire. Vous pouvez utiliser ce préfixe pour regrouper tous les fichiers de liste d'inventaire dans un emplacement commun au sein du compartiment de destination.
- *amzn-s3-demo-source-bucket* est le compartiment source pour lequel la liste d'inventaire est effectuée. Le nom du compartiment source est ajouté pour éviter les collisions lorsque plusieurs rapports d'inventaire de différents compartiments source sont envoyés dans le même compartiment de destination.
- *example-file-name*`.csv.gz` est l'un des fichiers de l'inventaire CSV. Les noms d'inventaire ORC se terminent par l'extension de nom de fichier `.orc` et les noms d'inventaire Parquet se terminent par l'extension de nom de fichier `.parquet`.

Manifeste d'inventaire

Les fichiers manifestes `manifest.json` et `symlink.txt` décrivent l'emplacement où les fichiers d'inventaire sont situés. Lorsqu'une nouvelle liste d'inventaire est fournie, elle est accompagnée d'un nouvel ensemble de fichiers manifestes. Ces fichiers peuvent s'écraser les uns les autres. Dans les compartiments activés pour la gestion des versions, Amazon S3 crée de nouvelles versions des fichiers de manifeste.

Chaque manifeste contenu dans le fichier `manifest.json` fournit des métadonnées et d'autres informations de base sur un inventaire. Les informations collectées sont les suivantes :

- Nom de compartiment source
- Nom du compartiment de destination
- Version de l'inventaire
- Horodatage de création, au format de date d'époque, composé de l'heure de début et de la date à laquelle le processus de génération de rapport d'inventaire a commencé à analyser le compartiment
- Format et schéma des fichiers d'inventaire

- Liste des fichiers d'inventaire se trouvant dans le compartiment de destination

Chaque fois qu'un `manifest.json` fichier est écrit, il est accompagné d'un `manifest.checksum` fichier qui est le MD5 hachage du contenu du `manifest.json` fichier.

Example Manifeste d'inventaire dans un fichier **`manifest.json`**

Voici des exemples de manifeste d'inventaire dans un fichier `manifest.json` pour les inventaires au format CSV, ORC et Parquet.

CSV

Voici un exemple de manifeste dans un fichier `manifest.json` pour un inventaire au format CSV.

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-inventory-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "CSV",
    "fileSchema": "Bucket, Key, VersionId, IsLatest, IsDeleteMarker,
 Size, LastModifiedDate, ETag, StorageClass, IsMultipartUploaded,
 ReplicationStatus, EncryptionStatus, ObjectLockRetainUntilDate, ObjectLockMode,
 ObjectLockLegalHoldStatus, IntelligentTieringAccessTier, BucketKeyStatus,
 ChecksumAlgorithm, ObjectAccessControlList, ObjectOwner",
    "files": [
        {
            "key": "Inventory/amzn-s3-demo-source-bucket/2016-11-06T21-32Z/
files/939c6d46-85a9-4ba8-87bd-9db705a579ce.csv.gz",
            "size": 2147483647,
            "MD5checksum": "f11166069f1990abeb9c97ace9cdfabc"
        }
    ]
}
```

ORC

Voici un exemple de manifeste dans un fichier `manifest.json` pour un inventaire au format ORC.

```
{
```

```
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "ORC",
    "fileSchema":
 "struct<bucket:string,key:string,version_id:string,is_latest:boolean,is_delete_marker:boole
    "files": [
        {
            "key": "inventory/amzn-s3-demo-source-bucket/data/
d794c570-95bb-4271-9128-26023c8b4900.orc",
            "size": 56291,
            "MD5checksum": "5925f4e78e1695c2d020b9f6eexample"
        }
    ]
}
```

Parquet

Voici un exemple de manifeste dans un fichier `manifest.json` pour un inventaire au format Parquet.

```
{
    "sourceBucket": "amzn-s3-demo-source-bucket",
    "destinationBucket": "arn:aws:s3:::example-destination-bucket",
    "version": "2016-11-30",
    "creationTimestamp" : "1514944800000",
    "fileFormat": "Parquet",
    "fileSchema": "message s3.inventory { required binary bucket (UTF8);
 required binary key (UTF8); optional binary version_id (UTF8); optional boolean
 is_latest; optional boolean is_delete_marker; optional int64 size; optional
 int64 last_modified_date (TIMESTAMP_MILLIS); optional binary e_tag (UTF8);
 optional binary storage_class (UTF8); optional boolean is_multipart_uploaded;
 optional binary replication_status (UTF8); optional binary encryption_status
 (UTF8); optional int64 object_lock_retain_until_date (TIMESTAMP_MILLIS); optional
 binary object_lock_mode (UTF8); optional binary object_lock_legal_hold_status
 (UTF8); optional binary intelligent_tiering_access_tier (UTF8); optional binary
 bucket_key_status (UTF8); optional binary checksum_algorithm (UTF8); optional
 binary object_access_control_list (UTF8); optional binary object_owner (UTF8);}",
    "files": [
        {
           "key": "inventory/amzn-s3-demo-source-bucket/data/
d754c470-85bb-4255-9218-47023c8b4910.parquet",
```

```
            "size": 56291,
            "MD5checksum": "5825f2e18e1695c2d030b9f6eexample"
        }
    ]
}
```

Le fichier `symlink.txt` est un fichier manifeste compatible avec Apache Hive qui permet à Hive de découvrir automatiquement les fichiers d'inventaire et leurs fichiers de données associés. Le manifeste compatible avec Hive fonctionne avec les services Athena et Amazon Redshift Spectrum compatibles avec Hive. Il fonctionne également avec les applications compatibles avec Hive, notamment Presto, Apache Hive, Apache Spark et bien d'autres applications.

> **Important**
>
> Le fichier manifeste compatible avec `symlink.txt` Apache Hive ne fonctionne pas avec AWS Glue actuellement.
> La lecture du fichier `symlink.txt` avec Apache Hive et Apache Spark n'est pas prise en charge par les fichiers d'inventaire au format ORC ou Parquet.

Configuration des notifications d'événements Amazon S3 pour l'achèvement de l'inventaire

Vous pouvez configurer une notification d'événement Amazon S3 afin de recevoir une notification lorsque le fichier du total de contrôle manifeste est créé, ce qui indique qu'une liste d'inventaire a été ajoutée au compartiment de destination. Le manifeste est une up-to-date liste de toutes les listes d'inventaire disponibles sur le site de destination.

Amazon S3 peut publier des événements dans une rubrique Amazon Simple Notification Service (Amazon SNS), une file d'attente Amazon Simple Queue Service (Amazon SQS) ou une fonction AWS Lambda . Pour plus d'informations, consultez Notifications d'événements Amazon S3.

La configuration de notification suivante définit que tous les fichiers `manifest.checksum` nouvellement ajoutés au compartiment de destination sont traités par l'opération AWS Lambda `cloud-function-list-write`.

```
<NotificationConfiguration>
  <QueueConfiguration>
```

```
      <Id>1</Id>
      <Filter>
          <S3Key>
              <FilterRule>
                  <Name>prefix</Name>
                  <Value>destination-prefix/source-bucket</Value>
              </FilterRule>
              <FilterRule>
                  <Name>suffix</Name>
                  <Value>checksum</Value>
              </FilterRule>
          </S3Key>
      </Filter>
      <CloudFunction>arn:aws:lambda:us-west-2:222233334444:cloud-function-list-write</
CloudFunction>
      <Event>s3:ObjectCreated:*</Event>
  </QueueConfiguration>
  </NotificationConfiguration>
```

Pour plus d'informations, consultez la section Utilisation AWS Lambda avec Amazon S3 dans le manuel du AWS Lambda développeur.

Interrogation d'un inventaire Amazon S3 avec Amazon Athena

Vous pouvez interroger les fichiers de l'inventaire Amazon S3 en utilisant des requêtes SQL standard à l'aide d'Amazon Athena dans toutes les Régions où Athena est disponible. Pour vérifier Région AWS la disponibilité, consultez le Région AWS tableau.

Athena peut interroger les fichiers d'inventaire Amazon S3 dans des colonnes de ligne optimisées (ORC) Apache, Apache Parquet ou au format CSV (valeurs séparées par des virgules). Lorsque vous utilisez Athena pour interroger les fichiers d'inventaire, nous vous recommandons d'utiliser des fichiers d'inventaire au format ORC ou Parquet. Les formats ORC et Parquet offrent des performances de requête plus rapides et des coûts de requête réduits. Les formats ORC et Parquet sont des formats auto-descriptifs en colonnes avec prise en charge du type, conçus pour Apache Hadoop. Le format en colonnes permet de lire, décompresser et traiter uniquement les colonnes nécessaires pour traiter la requête actuelle. L'ORC et les Parquet formats d'Amazon S3 Inventory sont disponibles dans tous les Régions AWS pays.

Pour utiliser Athena pour interroger les fichiers d'inventaire Amazon S3

1. Créez une table Athéna. Pour de plus amples informations sur la création d'une table, consultez Création de tables dans Athena dans le Guide de l'utilisateur Amazon Athena.
2. Créez votre requête à l'aide de l'un des exemples de modèles de requête suivants, selon que vous interrogez un rapport d'inventaire au format ORC, Parquet ou CSV.

   - Lorsque vous utilisez Athena pour interroger un rapport d'inventaire au format CSV, utilisez l'exemple de requête suivant en tant que modèle.

     L'exemple de requête suivant comprend tous les champs facultatifs dans le rapport d'inventaire au format ORC.

     Pour utiliser cet exemple de requête, procédez comme suit :

     - Remplacez *your_table_name* par le nom de la table Athena que vous avez créée.
     - Supprimez les champs facultatifs que vous n'avez pas choisis pour votre inventaire afin que la requête corresponde aux champs sélectionnés pour celui-ci.
     - Remplacez le nom de compartiment et l'emplacement d'inventaire (l'ID de configuration) suivants en fonction de votre configuration.

       `s3://`*amzn-s3-demo-bucket*`/`*config-ID*`/hive/`

     - Remplacez la date *2022-01-01-00-00* sous `projection.dt.range` par le premier jour de la plage horaire au cours de laquelle vous partitionnez les données dans Athena. Pour plus d'informations, consultez Partitionnement de données dans Athena.

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
         key string,
         version_id string,
         is_latest boolean,
         is_delete_marker boolean,
         size bigint,
         last_modified_date timestamp,
         e_tag string,
         storage_class string,
         is_multipart_uploaded boolean,
         replication_status string,
         encryption_status string,
         object_lock_retain_until_date bigint,
         object_lock_mode string,
```

```
         object_lock_legal_hold_status string,
         intelligent_tiering_access_tier string,
         bucket_key_status string,
         checksum_algorithm string,
         object_access_control_list string,
         object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.orc.OrcSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

- Lorsque vous utilisez Athena pour interroger un rapport d'inventaire au format Parquet, utilisez l'exemple de requête pour un rapport au format ORC. Toutefois, utilisez ce qui suit Parquet SerDe à la place de l'ORC SerDe dans la `ROW FORMAT SERDE` déclaration.

  ```
  ROW FORMAT SERDE 'org.apache.hadoop.hive.ql.io.parquet.serde.ParquetHiveSerDe'
  ```

- Lorsque vous utilisez Athena pour interroger un rapport d'inventaire au format CSV, utilisez l'exemple de requête suivant en tant que modèle.

  L'exemple de requête suivant comprend tous les champs facultatifs dans le rapport d'inventaire au format CSV.

  Pour utiliser cet exemple de requête, procédez comme suit :

  - Remplacez *`your_table_name`* par le nom de la table Athena que vous avez créée.
  - Supprimez les champs facultatifs que vous n'avez pas choisis pour votre inventaire afin que la requête corresponde aux champs sélectionnés pour celui-ci.
  - Remplacez le nom de compartiment et l'emplacement d'inventaire (l'ID de configuration) suivants en fonction de votre configuration.

s3://*amzn-s3-demo-bucket*/*config-ID*/hive/

- Remplacez la date *2022-01-01-00-00* sous `projection.dt.range` par le premier jour de la plage horaire au cours de laquelle vous partitionnez les données dans Athena. Pour plus d'informations, consultez Partitionnement de données dans Athena.

```
CREATE EXTERNAL TABLE your_table_name(
         bucket string,
         key string,
         version_id string,
         is_latest boolean,
         is_delete_marker boolean,
         size string,
         last_modified_date string,
         e_tag string,
         storage_class string,
         is_multipart_uploaded boolean,
         replication_status string,
         encryption_status string,
         object_lock_retain_until_date string,
         object_lock_mode string,
         object_lock_legal_hold_status string,
         intelligent_tiering_access_tier string,
         bucket_key_status string,
         checksum_algorithm string,
         object_access_control_list string,
         object_owner string
) PARTITIONED BY (
        dt string
)
ROW FORMAT SERDE 'org.apache.hadoop.hive.serde2.OpenCSVSerde'
  STORED AS INPUTFORMAT 'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat'
  OUTPUTFORMAT 'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat'
  LOCATION 's3://source-bucket/config-ID/hive/'
  TBLPROPERTIES (
    "projection.enabled" = "true",
    "projection.dt.type" = "date",
    "projection.dt.format" = "yyyy-MM-dd-HH-mm",
    "projection.dt.range" = "2022-01-01-00-00,NOW",
    "projection.dt.interval" = "1",
    "projection.dt.interval.unit" = "HOURS"
  );
```

3. Vous pouvez désormais exécuter différentes requêtes sur votre inventaire, comme le montrent les exemples suivants. Remplacez chaque *user input placeholder* par vos propres informations.

```
# Get a list of the latest inventory report dates available.
SELECT DISTINCT dt FROM your_table_name ORDER BY 1 DESC limit 10;

# Get the encryption status for a provided report date.
SELECT encryption_status, count(*) FROM your_table_name WHERE dt = 'YYYY-MM-DD-HH-
MM' GROUP BY encryption_status;

# Get the encryption status for inventory report dates in the provided range.
SELECT dt, encryption_status, count(*) FROM your_table_name
WHERE dt > 'YYYY-MM-DD-HH-MM' AND dt < 'YYYY-MM-DD-HH-MM' GROUP BY dt,
 encryption_status;
```

Lorsque vous configurez l'inventaire S3 pour ajouter le champ Liste de contrôle d'accès d'objet (Liste ACL d'objet) à un rapport d'inventaire, le rapport affiche la valeur du champ Liste ACL d'objet sous la forme d'une chaîne codée en base64. Pour obtenir la valeur décodée au format JSON pour le champ Liste ACL d'objet, vous pouvez interroger ce champ avec Athena. Consultez les exemples de requête suivants. Pour plus d'informations sur le champ Liste ACL d'objet, consultez Utiliser le champ Liste ACL d'objet.

```
# Get the S3 keys that have Object ACL grants with public access.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'uri') = 'http://acs.amazonaws.com/groups/global/AllUsers'
```

```
# Get the S3 keys that have Object ACL grantees in addition to the object owner.
WITH grants AS
```

```
    (SELECT key,
    from_utf8(from_base64(object_access_control_list)) AS
 object_access_control_list,
         object_owner,
         CAST(json_extract(from_utf8(from_base64(object_access_control_list)),
         '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))) AS grants_array
    FROM your_table_name)
SELECT key,
       grant,
       objectowner
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE cardinality(grants_array) > 1 AND element_at(grant, 'canonicalId') !=
 object_owner;
```

```
# Get the S3 keys with READ permission that is granted in the Object ACL.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'permission') = 'READ';
```

```
# Get the S3 keys that have Object ACL grants to a specific canonical user ID.
WITH grants AS (
    SELECT key,
        CAST(
            json_extract(from_utf8(from_base64(object_access_control_list)),
 '$.grants') AS ARRAY(MAP(VARCHAR, VARCHAR))
        ) AS grants_array
    FROM your_table_name
)
SELECT key,
       grants_array,
```

```
       grant
FROM grants, UNNEST(grants_array) AS t(grant)
WHERE element_at(grant, 'canonicalId') = 'user-canonical-id';
```

```
# Get the number of grantees on the Object ACL.
SELECT key,
       object_access_control_list,
       json_array_length(json_extract(object_access_control_list,'$.grants')) AS
 grants_count
FROM your_table_name;
```

Pour plus d'informations sur l'utilisation d'Athena, consultez le Guide de l'utilisateur Amazon Athena.

Conversion de chaînes d'ID de version vides dans les rapports d'inventaire Amazon S3 en chaînes null

> **Note**
>
> La procédure suivante s'applique uniquement aux rapports d'inventaire Amazon S3 qui incluent toutes les versions, et uniquement si les rapports « toutes les versions » sont utilisés comme manifestes pour S3 Batch Operations sur des compartiments sur lesquels la gestion des versions S3 est activée. Il n'est pas nécessaire de convertir des chaînes pour les rapports d'inventaire S3 qui spécifient uniquement la version actuelle.

Vous pouvez utiliser les rapports d'inventaire S3 en tant que manifestes pour S3 Batch Operations. Toutefois, si la gestion des versions S3 est activée sur un compartiment, les rapports d'inventaire S3 qui incluent toutes les versions marquent tous les objets versionnés NULL avec des chaînes vides dans le champ d'ID de version. Lorsqu'un rapport d'inventaire inclut toutes les versions de l'objet IDs, Batch Operations reconnaît `null` les chaînes comme des versions IDs, mais pas les chaînes vides.

Si une tâche S3 Batch Operations utilise un rapport d'inventaire S3 « toutes les versions » comme manifeste, il échoue toutes les tâches sur les objets dont la chaîne est vide dans le champ d'ID de version. Pour convertir des chaînes vides dans le champ d'ID de version du rapport d'inventaire S3 en chaînes `null` pour Batch Operations, suivez la procédure suivante.

Mise à jour d'un rapport d'inventaire Amazon S3 pour l'utiliser avec Batch Operations

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Accédez à votre rapport d'inventaire S3. Le rapport d'inventaire se trouve dans le compartiment de destination que vous avez spécifié lors de la configuration de votre rapport d'inventaire. Pour de plus amples informations sur la manière de trouver les rapports d'inventaire, consultez Localisation de votre liste d'inventaire.

   a. Choisissez le compartiment de destination.

   b. Choisissez le dossier. Le dossier porte le nom du compartiment source d'origine.

   c. Choisissez le dossier nommé d'après la configuration d'inventaire.

   d. Cochez la case en regard du dossier nommé hive. En haut de la page, choisissez Copy S3 URI (Copier l'URI S3) pour copier l'URI S3 du dossier.
3. Ouvrez la console Amazon Athena à l'adresse. https://console.aws.amazon.com/athena/
4. Dans l'éditeur de requête, choisissez Settings (Paramètres), puis Manage (Gérer). Sur la page Manage settings (Gérer les paramètres), pour Location of query result (Emplacement des résultats de la requête), choisissez un compartiment S3 dans lequel stocker les résultats de votre requête.
5. Dans l'éditeur de requête, créez une table Athena pour contenir les données du rapport d'inventaire à l'aide de la commande suivante. Remplacez *table_name* par un nom de votre choix, et dans la clause `LOCATION`, insérez l'URI S3 que vous avez copié précédemment. Choisissez ensuite Run (Exécuter) pour exécuter la requête.

   ```
   CREATE EXTERNAL TABLE table_name(bucket string, key string,
    version_id string) PARTITIONED BY (dt string)ROW FORMAT SERDE
    'org.apache.hadoop.hive.serde2.OpenCSVSerde'STORED AS INPUTFORMAT
    'org.apache.hadoop.hive.ql.io.SymlinkTextInputFormat' OUTPUTFORMAT
    'org.apache.hadoop.hive.ql.io.IgnoreKeyTextOutputFormat' LOCATION 'Copied S3 URI';
   ```
6. Pour effacer l'éditeur de requête, cliquez sur Clear (Effacer). Ensuite, chargez le rapport d'inventaire dans la table à l'aide de la commande suivante. Remplacez *table_name* par le nom que vous avez choisi lors de l'étape précédente. Choisissez ensuite Run (Exécuter) pour exécuter la requête.

   ```
   MSCK REPAIR TABLE table_name;
   ```

7. Pour effacer l'éditeur de requête, cliquez sur Clear (Effacer). Exécutez la `SELECT` requête suivante pour récupérer toutes les entrées du rapport d'inventaire d'origine et remplacez toute version vide par IDs des `null` chaînes. Remplacez *`table_name`* par le nom que vous avez choisi précédemment, et remplacez *`YYYY-MM-DD-HH-MM`* dans la clause `WHERE` par la date du rapport d'inventaire à laquelle vous souhaitez que cet outil soit exécuté. Choisissez ensuite Run (Exécuter) pour exécuter la requête.

```
SELECT bucket as Bucket, key as Key, CASE WHEN version_id = '' THEN 'null' ELSE
 version_id END as VersionId FROM table_name WHERE dt = 'YYYY-MM-DD-HH-MM';
```

8. Retournez à la console Amazon S3 (https://console.aws.amazon.com/s3/) et accédez au compartiment S3 que vous avez choisi pour Emplacement du résultat de la requête plus tôt. Il devrait contenir une série de dossiers se terminant par la date.

   Par exemple, vous devriez voir quelque chose comme s3 ://***amzn-s3-demo-bucket***/***query-result-location***/Unsaved/2021/10/07/. Vous devriez voir des fichiers `.csv` contenant les résultats de la requête `SELECT` que vous avez exécutée.

   Choisissez le fichier CSV avec la date de modification la plus récente. Téléchargez ce fichier sur votre ordinateur local pour la prochaine étape.

9. Le fichier CSV généré contient une ligne d'en-tête. Pour utiliser ce fichier CSV en tant qu'entrée pour une tâche S3 Batch Operations, vous devez supprimer la ligne d'en-tête, car Batch Operations ne prend pas en charge les lignes d'en-tête sur les manifestes CSV.

   Pour supprimer la ligne d'en-tête, vous pouvez exécuter l'une des commandes suivantes sur le fichier. Remplacez *`file.csv`* par le nom de votre fichier CSV.

   Pour les machines macOS et Linux, exécutez la commande `tail` dans une fenêtre Terminal.

```
tail -n +2 file.csv > tmp.csv && mv tmp.csv file.csv
```

   Pour les machines Windows, exécutez le script suivant dans une PowerShell fenêtre Windows. Remplacez *`File-location`* par le chemin de votre fichier et *`file.csv`* par le nom du fichier.

```
$ins = New-Object System.IO.StreamReader File-location\file.csv
$outs = New-Object System.IO.StreamWriter File-location\temp.csv
try {
    $skip = 0
    while ( !$ins.EndOfStream ) {
```

```
        $line = $ins.ReadLine();
        if ( $skip -ne 0 ) {
            $outs.WriteLine($line);
        } else {
            $skip = 1
        }
    }
} finally {
    $outs.Close();
    $ins.Close();
}
Move-Item File-location\temp.csv File-location\file.csv -Force
```

10. Après avoir supprimé la ligne d'en-tête du fichier CSV, vous êtes prêt à utiliser ce dernier comme manifeste dans une tâche S3 Batch Operations. Chargez le fichier CSV dans un compartiment S3 ou un emplacement de votre choix, puis créez une tâche Batch Operations en utilisant le fichier CSV comme manifeste.

    Pour de plus amples informations sur la création d'une tâche Batch Operations, consultez Création d'une tâche d'opérations par lot S3.

Utiliser le champ Liste ACL d'objet

Un rapport d'inventaire Amazon S3 contient une liste des objets figurant dans le compartiment source S3 et les métadonnées de chaque objet. Le champ Liste de contrôle d'accès (ACL) d'objet est un champ de métadonnées disponible dans l'inventaire Amazon S3. Plus précisément, le champ Liste ACL d'objet contient la liste de contrôle d'accès (ACL) de chaque objet. L'ACL d'un objet définit le Comptes AWS ou les groupes autorisés à accéder à cet objet et le type d'accès accordé. Pour plus d'informations, consultez Présentation de la liste de contrôle d'accès (ACL) et Liste d'inventaire Amazon S3.

Le champ Liste ACL de l'objet dans les rapports d'inventaire Amazon S3 est défini au format JSON. Les données JSON comprennent les champs suivants :

- `version` : version du format de champ Liste ACL de l'objet dans les rapports d'inventaire. Ce champ possède le format de date `yyyy-mm-dd`.
- `status` : les valeurs possibles sont `AVAILABLE` ou `UNAVAILABLE` pour indiquer si une liste ACL d'objet est disponible pour un objet. Lorsque le statut de la liste ACL de l'objet est `UNAVAILABLE`, la valeur du champ Propriétaire de l'objet dans le rapport d'inventaire est également `UNAVAILABLE`.

- `grants` : paires bénéficiaire-autorisation qui répertorient le statut d'autorisation de chaque bénéficiaire accordé par la liste ACL de l'objet. Les valeurs disponibles pour un bénéficiaire sont `CanonicalUser` et `Group`. Pour plus d'informations sur les bénéficiaires, consultez Bénéficiaires figurant dans les listes de contrôle d'accès.

  Pour un bénéficiaire possédant le type `Group`, une paire bénéficiaire-autorisation inclut les attributs suivants :

  - `uri` : un groupe Amazon S3 prédéfini.
  - `permission` : les autorisations de liste ACL accordées sur l'objet. Pour plus d'informations, consultez Autorisations de liste ACL sur un objet.
  - `type` : le type `Group`, qui indique que le bénéficiaire est un groupe.

  Pour un bénéficiaire possédant le type `CanonicalUser`, une paire bénéficiaire-autorisation inclut les attributs suivants :

  - `canonicalId` : une forme obfusquée de l'ID Compte AWS . L'ID utilisateur canonique d'un Compte AWS est spécifique à ce compte. Vous pouvez récupérer l'ID d'utilisateur canonique. Pour plus d'informations, consultez la section Trouver le nom d'utilisateur canonique correspondant à votre compte Compte AWS dans le Guide de référence de gestion de AWS compte.

    > **Note**
    >
    > Si le bénéficiaire d'une ACL est l'adresse e-mail d'un Compte AWS, S3 Inventory utilise cette adresse Compte AWS et le `CanonicalUser` type pour spécifier ce bénéficiaire. `canonicalId` Pour plus d'informations, consultez Bénéficiaires figurant dans les listes de contrôle d'accès.

  - `permission` : les autorisations de liste ACL accordées sur l'objet. Pour plus d'informations, consultez Autorisations de liste ACL sur un objet.
  - `type`— Le type`CanonicalUser`, qui indique que le bénéficiaire est un. Compte AWS

L'exemple suivant montre les valeurs possibles pour le champ Liste ACL d'objet au format JSON :

```
{
    "version": "2022-11-10",
    "status": "AVAILABLE",
    "grants": [{
```

```
        "uri": "http://acs.amazonaws.com/groups/global/AllUsers",
        "permission": "READ",
        "type": "Group"
    }, {
        "canonicalId": "example-canonical-id",
        "permission": "FULL_CONTROL",
        "type": "CanonicalUser"
    }]
}
```

Note

Le champ Liste ACL d'objet est défini au format JSON. Un rapport d'inventaire affiche la valeur du champ Liste ACL d'objet sous la forme d'une chaîne codée en base64. Supposons, par exemple, que vous disposiez du champ Liste ACL d'objet suivant au format JSON :

```
{
        "version": "2022-11-10",
        "status": "AVAILABLE",
        "grants": [{
            "canonicalId": "example-canonical-user-ID",
            "type": "CanonicalUser",
            "permission": "READ"
        }]
}
```

Le champ Liste ACL d'objet est codé et affiché sous la forme de la chaîne codée en base64 suivante :

```
eyJ2ZXJzaW9uIjoiMjAyMi0xMS0xMCIsInN0YXR1cyI6IkFWQUlMQUJMRSIsImdyYW50cyI6W3siY2Fub25pY2FsSW
```

Pour obtenir la valeur décodée au format JSON pour le champ Liste ACL d'objet, vous pouvez interroger ce champ dans Amazon Athena. Pour d'autres exemples de requête, consultez Interrogation d'un inventaire Amazon S3 avec Amazon Athena.

Modèles de conception des bonnes pratiques : optimisation des performances d'Amazon S3

Vos applications peuvent facilement exécuter des milliers de transactions par seconde lors du chargement et de l'extraction du stockage depuis Amazon S3. Amazon S3 se met automatiquement à l'échelle en fonction des taux de demandes très importants. Par exemple, votre application peut traiter au moins 3 500 PUT/COPY/POST/DELETE or 5,500 GET/HEAD demandes par seconde par préfixe Amazon S3 partitionné. Il n'existe aucune limite au nombre de préfixes dans un compartiment. Vous pouvez augmenter vos performances de lecture et d'écriture en effectuant une mise en parallèle. Par exemple, si vous créez 10 préfixes dans un compartiment Amazon S3 pour paralléliser les lectures, vous pouvez adapter vos performances de lecture à 55 000 demandes de lecture par seconde. De même, vous pouvez mettre à l'échelle les opérations d'écriture en écrivant sur plusieurs préfixes. La mise à l'échelle, dans le cas des opérations de lecture et d'écriture, se fait progressivement et n'est pas instantanée, et les performances réelles varient en fonction des caractéristiques spécifiques de votre charge de travail, de vos modèles d'utilisation et de la configuration du système. Pendant la mise à l'échelle d'Amazon S3 à votre nouveau taux de demandes plus élevé, vous pouvez rencontrer des erreurs 503 (Ralentissement). Ces erreurs disparaissent une fois la mise à l'échelle terminée. Pour plus d'informations sur la création et l'utilisation de préfixes, consultez Organisation des objets à l'aide de préfixes.

Certaines applications de lacs de données sur Amazon S3 analysent des milliards d'objets pour les requêtes qui portent sur des péta-octets de données. Ces applications de lac de données atteignent des taux de transfert en instance unique qui maximisent l'utilisation de l'interface réseau pour leur EC2 instance Amazon, qui peut atteindre 100 Gb/s sur une seule instance. Ces applications regroupent ensuite le débit de plusieurs instances pour parvenir à plusieurs téraoctets par seconde.

D'autres applications sont sensibles à la latence, comme les applications de messagerie des réseaux sociaux. Ces applications peuvent atteindre des latences constantes pour les petits objets (et les first-byte-out latences pour les objets plus grands) d'environ 100 à 200 millisecondes.

D'autres AWS services peuvent également contribuer à accélérer les performances de différentes architectures d'applications. Par exemple, si vous souhaitez des taux de transfert plus élevés sur une seule connexion HTTP ou des latences à un chiffre en millisecondes, utilisez Amazon CloudFront ou Amazon pour la mise en cache avec ElastiCacheAmazon S3.

De plus, si vous souhaitez un transport rapide de données sur de longues distances entre un client et un compartiment S3, utilisez Configuration de transferts de fichiers rapides et sécurisés à l'aide

d'Amazon S3 Transfer Acceleration. Transfer Acceleration utilise les emplacements périphériques répartis dans le monde entier CloudFront pour accélérer le transport des données sur des distances géographiques. Si votre charge de travail Amazon S3 utilise le chiffrement côté serveur avec AWS KMS, consultez la section AWS KMS Limites du guide du AWS Key Management Service développeur pour obtenir des informations sur les taux de demandes pris en charge pour votre cas d'utilisation.

Les rubriques suivantes décrivent les instructions et les modèles de conception des bonnes pratiques pour optimiser les performances des applications qui utilisent Amazon S3. Veuillez consulter Recommandations de performance pour Amazon S3 et Modèles de conception des performances pour Amazon S3 pour obtenir les informations les plus à jour sur l'optimisation des performances pour Amazon S3.

> **Note**
>
> Pour plus d'informations sur l'utilisation de la classe de stockage Amazon S3 Express One Zone avec des compartiments de répertoires, consultez S3 Express One Zone et Utilisation des compartiments de répertoires.

Rubriques

- Recommandations de performance pour Amazon S3
- Modèles de conception des performances pour Amazon S3

Recommandations de performance pour Amazon S3

Lors du développement d'applications qui téléchargent et extraient les objets depuis Amazon S3, suivez nos instructions sur les bonnes pratiques pour optimiser les performances. Nous proposons également des Modèles de conception des performances pour Amazon S3 plus détaillés.

Pour obtenir les meilleures performances pour votre application sur Amazon S3, nous recommandons les directives suivantes.

Rubriques

- Mesurer les performances

- Mise à l'échelle horizontale des connexions de stockage
- Utilisation des extractions de plages d'octets
- Nouvelle tentative de demandes pour les applications sensibles à la latence
- Combinez Amazon S3 (stockage) et Amazon EC2 (calcul) en un seul Région AWS
- Utilisation d'Amazon S3 Transfer Acceleration pour réduire la latence provoquée par la distance
- Utilisez la dernière version du AWS SDKs

Mesurer les performances

Lors de l'optimisation des performances, examinez le débit du réseau, l'UC et les exigences DRAM. En fonction de la combinaison des demandes pour ces différentes ressources, il peut être utile d'évaluer différents types d' EC2instances Amazon. Pour plus d'informations sur les types d'instances, consultez la section Types d'instances dans le guide de EC2 l'utilisateur Amazon.

Il peut aussi être utile d'examiner le temps de recherche DNS, la latence et la vitesse de transfert des données à l'aide des outils d'analyse HTTP lors de la mesure des performances.

Pour comprendre les exigences de performances et optimiser les performances de votre application, vous pouvez également surveiller les réponses d'erreur 503 que vous recevez. La surveillance de certaines métriques de performances peut entraîner des dépenses supplémentaires. Pour plus d'informations, consultez Tarification Amazon S3.

Surveillance du nombre de réponses d'erreur de statut 503 (Ralentissement)

Pour surveiller le nombre de réponses d'erreur de statut 503 que vous recevez, vous pouvez utiliser l'une des options suivantes :

- Utilisez les métriques de CloudWatch demande Amazon pour Amazon S3. Les métriques de CloudWatch demande incluent une métrique pour les réponses d'état 5xx. Pour plus d'informations sur les métriques de demande CloudWatch , consultez Surveillance des métriques avec Amazon CloudWatch.
- Utilisez le nombre d'erreurs 503 (Service non disponible) disponible dans la section des métriques avancées d'Amazon S3 Storage Lens. Pour plus d'informations, consultez Utilisation de métriques S3 Storage Lens pour améliorer les performances.
- Utilisez la journalisation des accès au serveur Amazon S3. La journalisation des accès au serveur vous permet de filtrer et de passer en revue toutes les demandes qui reçoivent des réponses 503 (Erreur interne). Vous pouvez également utiliser Amazon Athena pour analyser les journaux. Pour

en savoir plus sur la journalisation des accès au serveur, consultez Enregistrement de demandes avec journalisation des accès au serveur.

En surveillant le nombre de codes d'erreur de statut HTTP 503, vous pouvez souvent obtenir des insights précieux sur les préfixes, les clés ou les compartiments qui reçoivent le plus de demandes de limitation.

Mise à l'échelle horizontale des connexions de stockage

La répartition des demandes entre plusieurs connexions est un modèle de conception courant pour mettre horizontalement à l'échelle les performances. Lorsque vous développez des applications hautes performances, pensez à Amazon S3 comme à un très grand système réparti, et non comme un simple point de terminaison réseau, tel qu'un serveur de stockage traditionnel. Vous pouvez atteindre les meilleures performances en adressant plusieurs demandes concurrentes à Amazon S3. Répartissez ces demandes sur des connexions distinctes pour maximiser la bande passante accessible à partir d'Amazon S3. Amazon S3 n'a aucune limite pour le nombre de connexions à votre compartiment.

Utilisation des extractions de plages d'octets

Avec l'en-tête HTTP `Range` dans une demande GET Object, vous pouvez extraire une plage d'octets d'un objet, en ne transférant que la portion spécifiée. Vous pouvez utiliser des connexions simultanées vers Amazon S3 pour extraire différentes plages d'octets depuis le même objet. Vous pouvez ainsi parvenir au regroupement de débits le plus élevé, par opposition à une seule demande d'objet entier. L'extraction des plages les plus petites d'un grand objet permet aussi à votre application d'améliorer l'intervalle des nouvelles tentatives quand les demandes sont interrompues. Pour plus d'informations, consultez Téléchargement d'objets.

Les tailles traditionnelles des demandes de plages d'octets sont de 8 Mo ou 16 Mo. Si les objets sont l'objet d'une opération PUT à l'aide d'un chargement en plusieurs parties, une bonne pratique consiste à les soumettre à une opération GET dans les mêmes tailles d'élément (ou au moins alignées sur les frontières d'élément) pour obtenir de meilleures performances. Les demandes GET peuvent directement adresser les éléments individuels ; par exemple, `GET ?partNumber=N.`

Nouvelle tentative de demandes pour les applications sensibles à la latence

Les expirations et les nouvelles tentatives agressives permettent d'obtenir une latence cohérente. Étant donnée la large échelle d'Amazon S3, si la première demande est lente, une demande de

nouvelle tentative est susceptible d'emprunter un chemin différent et de réussir rapidement. Ils AWS SDKs ont des valeurs de délai d'expiration et de nouvelle tentative configurables que vous pouvez ajuster en fonction des tolérances de votre application spécifique.

Combinez Amazon S3 (stockage) et Amazon EC2 (calcul) en un seul Région AWS

Même si les noms de compartiment S3 sont globalement uniques, chaque compartiment est stocké dans une région que vous sélectionnez lorsque vous créez le compartiment. Pour en savoir plus sur les directives relatives à la dénomination des compartiments, consultez Présentation des compartiments et Règles de dénomination des compartiments. Pour optimiser les performances, nous vous recommandons d'accéder au bucket depuis les EC2 instances Amazon de la même manière Région AWS lorsque cela est possible. Cela permet de réduire la latence réseau et les coûts de transfert des données.

Pour plus d'informations sur la tarification du transfert des données, consultez la Tarification Amazon S3.

Utilisation d'Amazon S3 Transfer Acceleration pour réduire la latence provoquée par la distance

Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration permet un transfert rapide, facile et sécurisé des fichiers sur des longues distances entre votre client et un compartiment S3. Transfer Acceleration tire parti des emplacements périphériques répartis dans le monde entier sur Amazon CloudFront. Lorsque les données arrivent dans un emplacement périphérique, elles sont transférées vers Amazon S3 sur un chemin de réseau optimisé. Transfer Acceleration convient parfaitement au transfert régulier de gigaoctets ou téraoctets de données d'un continent à l'autre. Il est aussi utile pour les clients qui chargent sur un compartiment centralisé depuis le monde entier.

Vous pouvez utiliser l'outil de comparaison de vitesse Amazon S3 Transfer Acceleration pour comparer les vitesses de chargement accéléré et non accéléré dans les régions Amazon S3. L'outil de comparaison de la vitesse utilise les chargements partitionnés pour transférer un fichier à partir de votre navigateur vers différentes régions Amazon S3 avec ou sans Amazon S3 Transfer Acceleration.

Utilisez la dernière version du AWS SDKs

Ils AWS SDKs fournissent un support intégré pour de nombreuses directives recommandées pour optimiser les performances d'Amazon S3. Ils SDKs fournissent une API plus simple pour tirer parti

d'Amazon S3 depuis une application et sont régulièrement mis à jour pour suivre les meilleures pratiques les plus récentes. Par exemple, ils SDKs incluent une logique qui permet de réessayer automatiquement les requêtes en cas d'erreur HTTP 503 et d'investir dans du code pour répondre et s'adapter aux connexions lentes.

Ils fournissent SDKs également le gestionnaire de transfert, qui automatise le dimensionnement horizontal des connexions pour traiter des milliers de demandes par seconde, en utilisant des requêtes par plage d'octets le cas échéant. Il est important d'utiliser la dernière version du AWS SDKs pour obtenir les dernières fonctionnalités d'optimisation des performances.

Vous pouvez aussi optimiser les performances lorsque vous utilisez les demandes d'API REST HTTP. Lorsque vous utilisez l'API REST, vous devez suivre les mêmes bonnes pratiques que celles incluses dans le SDKs. Autorisez les délais d'expiration et les nouvelles tentatives sur les demandes lentes, et multipliez les connexions pour autoriser l'extraction de données d'objet en parallèle. Pour plus d'informations sur l'utilisation de l'API REST, consultez la Référence d'API Amazon Simple Storage Service.

Modèles de conception des performances pour Amazon S3

Lors de la conception d'applications pour télécharger et extraire des objets depuis Amazon S3, utilisez nos modèles de conception des bonnes pratiques pour parvenir aux meilleures performances de votre application. Nous vous proposons aussi de prendre en compte des Recommandations de performance pour Amazon S3 lors de la planification de l'architecture de votre application.

Pour optimiser les performances, vous pouvez utiliser les modèles de conception suivants.

Rubriques

- Utilisation de la mise en cache pour le contenu consulté fréquemment
- Délais d'expiration et nouvelles tentatives pour les applications sensibles à la latence
- Mise à l'échelle horizontale et mise en parallèle des demandes pour le haut débit
- Utilisation d'Amazon S3 Transfer Acceleration pour accélérer les transferts de données disparates géographiquement

Utilisation de la mise en cache pour le contenu consulté fréquemment

De nombreuses applications qui stockent des données dans Amazon S3 fournissent un « ensemble fonctionnel » de données demandé à plusieurs reprises par les utilisateurs. Si une charge de travail

envoie des requêtes GET répétées pour un ensemble commun d'objets, vous pouvez utiliser un cache tel qu'Amazon CloudFront ElastiCache, Amazon ou AWS Elemental MediaStorepour optimiser les performances. L'adoption réussie du cache peut se traduire par une latence faible et des taux élevés de transfert des données. Les applications qui utilisent la mise en cache envoient aussi moins de demandes directes à Amazon S3, ce qui peut aider à réduire les coûts des demandes.

Amazon CloudFront est un réseau de diffusion de contenu rapide (CDN) qui met en cache de manière transparente les données d'Amazon S3 dans un grand nombre de points de présence répartis géographiquement (). PoPs Lorsque des objets sont accessibles depuis plusieurs régions ou via Internet, cela CloudFront permet aux données d'être mises en cache à proximité des utilisateurs qui accèdent aux objets. Il peut en résulter une diffusion haute performance des contenus Amazon S3 réputés. Pour plus d'informations à ce sujet CloudFront, consultez le manuel Amazon CloudFront Developer Guide.

Amazon ElastiCache est un cache en mémoire géré. Avec ElastiCache, vous pouvez provisionner des EC2 instances Amazon qui mettent en cache des objets en mémoire. Cette mise en cache se traduit par des ordres de réduction de magnitude dans la latence GET et de substantielles augmentations dans le débit de téléchargement. Pour l'utiliser ElastiCache, vous modifiez la logique de l'application pour remplir le cache avec des objets chauds et vérifier la présence d'objets chauds dans le cache avant de les demander à Amazon S3. Pour des exemples d'utilisation visant ElastiCache à améliorer les performances GET d'Amazon S3, consultez le billet de blog Turbocharger Amazon S3 avec Amazon ElastiCache pour Redis.

AWS Elemental MediaStore est un système de mise en cache et de distribution de contenu spécialement conçu pour les flux de travail vidéo et la diffusion de contenu multimédia à partir d'Amazon S3. MediaStore fournit un end-to-end stockage APIs spécifique pour les vidéos et est recommandé pour les charges de travail vidéo sensibles aux performances. Pour plus d'informations MediaStore, consultez le guide de AWS Elemental MediaStore l'utilisateur.

Délais d'expiration et nouvelles tentatives pour les applications sensibles à la latence

Dans certaines situations, une application reçoit une réponse d'Amazon S3 indiquant qu'une nouvelle tentative est nécessaire. Amazon S3 mappe les noms de compartiment et d'objet aux données d'objet qui leur sont associées. Si une application génère des taux de demande élevés (généralement des taux soutenus de plus de 5 000 demandes par seconde pour un petit nombre d'objets), elle peut recevoir des réponses HTTP 503 slowdown. Si ces erreurs se produisent, chaque kit SDK AWS implémente une logique de nouvelle tentative automatique à l'aide d'une

interruption exponentielle. Si vous n'utilisez pas de kit SDK AWS , vous devez implémenter une logique de nouvelle tentative lors de la réception de l'erreur HTTP 503. Pour plus d'informations sur les techniques de réduction, consultez la section Comportement des nouvelles tentatives dans le guide de référence des outils AWS SDKs et.

Amazon S3 se met automatiquement à l'échelle en réponse aux taux soutenus de nouvelles demandes, optimisant dynamiquement les performances. Tandis qu'Amazon S3 optimise en interne le taux de nouvelles demandes, vous recevez temporairement des réponses HTTP 503 jusqu'à ce que l'optimisation soit terminée. Après qu'Amazon S3 optimise en interne les performances pour le nouveau taux de demandes, toutes les demandes sont généralement traitées sans nouvelles tentatives.

Pour les applications sensibles à la latence, Amazon S3 conseille un suivi et des opérations de nouvelles tentatives plus lentes. Lorsque vous retentez une demande, nous recommandons l'utilisation d'une nouvelle connexion à Amazon S3 et l'exécution d'une nouvelle recherche DNS.

Lorsque vous effectuez des demandes volumineuses de taille variable (par exemple, plus de 128 Mo), nous conseillons de suivre le débit obtenu et de procéder à de nouvelles tentatives sur les 5 % les plus lents des demandes. Lorsque vous exécutez des demandes plus petites (par exemple, inférieures à 512 Ko), où les latences médianes sont souvent dans une plage de dix millisecondes, une bonne instruction consiste à retenter une opération GET ou PUT après 2 secondes. Si de nouvelles tentatives sont nécessaires, la bonne pratique consiste à se retirer. Par exemple, nous recommandons de n'émettre une nouvelle tentative qu'après 2 secondes et une deuxième nouvelle tentative au bout de 4 secondes supplémentaires.

Si votre application adresse des demandes de taille fixe à Amazon S3, vous devez escompter des temps de réponse plus cohérents pour chacune de ces demandes. Dans ce cas, une stratégie simple consiste à identifier le 1 % de demandes les plus lentes et de les réessayer. Même une simple nouvelle tentative est fréquemment efficace pour réduire la latence.

Si vous utilisez AWS Key Management Service (AWS KMS) pour le chiffrement côté serveur, consultez la section Quotas du guide du AWS Key Management Service développeur pour obtenir des informations sur les taux de demandes pris en charge pour votre cas d'utilisation.

Mise à l'échelle horizontale et mise en parallèle des demandes pour le haut débit

Amazon S3 est un système distribué très large. Pour vous aider à tirer parti de son échelle, nous vous encourageons à horizontalement mettre à l'échelle les demandes parallèles adressées aux

points de terminaison du service Amazon S3. En plus de la distribution des demandes au sein d'Amazon S3, ce type d'approche de la mise à l'échelle permet de répartir la charge sur plusieurs chemins d'accès du réseau.

Pour les transferts à haut débit, Amazon S3 conseille l'utilisation d'applications employant plusieurs connexions pour exécuter des opérations GET ou PUT sur les données en parallèle. Par exemple, cela est pris en charge par Amazon S3 Transfer Manager dans le SDK AWS Java, et la plupart des autres AWS SDKs proposent des constructions similaires. Pour certaines applications, vous pouvez obtenir des connexions parallèles en lançant plusieurs demandes simultanément dans différents threads d'application ou dans différentes instances d'application. La meilleure approche à adopter dépend de votre application et de la structure des objets auxquels vous accédez.

Vous pouvez utiliser le AWS SDKs pour émettre directement des requêtes GET et PUT plutôt que d'utiliser la gestion des transferts dans le AWS SDK. Cette approche vous permet d'affiner votre charge de travail plus directement, tout en tirant profit du support du kit SDK pour les nouvelles tentatives et sa gestions des réponses HTTP 503 qui peuvent se produire. En règle générale, lorsque vous téléchargez des objets volumineux au sein d'une région depuis Amazon S3 vers Amazon EC2, nous vous suggérons de demander simultanément des plages d'octets d'un objet d'une granularité de 8 à 16 Mo. Effectuez une demande simultanée pour chaque tranche de 85 à 90 % MB/s du débit réseau souhaité. Pour saturer une carte d'interface Gb/s réseau (NIC) à 10 unités, vous pouvez utiliser environ 15 demandes simultanées sur des connexions distinctes. Vous pouvez augmenter le nombre de demandes simultanées sur un plus grand nombre de connexions pour les saturer plus rapidement NICs, par exemple 25 Gb/s ou 100 Gb/s NICs.

La mesure des performances est importante quand vous réglez le nombre de demandes à émettre simultanément. Il est recommandé de commencer avec une seule demande à la fois. Mesurez la bande passante réseau obtenue et l'utilisation des autres ressources que votre application utilise dans le traitement des données. Vous pouvez alors identifier la ressource du goulet d'étranglement (à savoir, la ressource avec l'utilisation la plus élevée), et de là le nombre de requêtes susceptibles d'être utiles. Par exemple, si le traitement d'une demande à la fois conduit à une utilisation de l'UC de 25 %, cela induit que quatre demandes simultanées au plus peuvent être accueillies. Les mesures sont essentielles et il vaut la peine de confirmer l'utilisation des ressources tandis que le taux des demandes augmente.

Si votre application adresse directement des demandes à Amazon S3 à l'aide de l'API REST, nous recommandons l'utilisation d'un groupe de connexions HTTP et la réutilisation de chaque connexion pour un ensemble de demandes. Le fait d'éviter la configuration des connexions par demande supprime la nécessité d'exécuter des liaisons TCP à démarrage lent et SSL (Secure Sockets Layer)

sur chaque demande. Pour plus d'informations sur l'utilisation de l'API REST, consultez la Référence d'API Amazon Simple Storage Service.

Enfin, il vaut la peine de prêter attention à DNS et de vérifier que les demandes sont réparties sur un vaste groupe d'adresses IP Amazon S3. Les requêtes DNS pour le Amazon S3 parcourent une large liste de points de terminaison IP. Mais la mise en cache des programmes de résolution ou du code d'application qui réutilise une seule adresse IP ne tire pas parti de la diversité des adresses et de l'équilibrage de charge qui en découle. Les outils d'utilitaire réseau comme l'outil de ligne de commande `netstat` peuvent afficher les adresses IP utilisées pour la communication avec Amazon S3 et nous fournissons des instructions sur les configurations DNS à utiliser. Pour plus d'informations sur ces directives, consultez Envoi de demandes dans la Référence d'API Amazon S3.

Utilisation d'Amazon S3 Transfer Acceleration pour accélérer les transferts de données disparates géographiquement

Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration est efficace pour réduire ou supprimer la latence provoquée par la distance géographique entre les clients dispersés géographiquement et une application régionale qui utilise Amazon S3. Transfer Acceleration utilise les emplacements périphériques répartis dans le monde entier CloudFront pour le transport des données. Le réseau AWS périphérique possède des points de présence dans plus de 50 sites. Aujourd'hui, il est utilisé pour distribuer du contenu via Amazon Route 53 CloudFront et pour fournir des réponses rapides aux requêtes DNS adressées à Amazon Route 53.

Le réseau périphérique aide également à accélérer les transferts de données dans et en dehors d'Amazon S3. Il convient parfaitement aux applications qui transfèrent les données entre les continents, ont une connexion Internet rapide, utilise des objets de grande taille ou ont un contenu volumineux à charger. Lorsque les données arrivent dans un emplacement périphérique, elles sont transférées vers Amazon S3 sur un chemin de réseau optimisé. En général, plus vous êtes loin d'une région Amazon S3, plus vous pouvez escompter une amélioration de la vitesse grâce à Transfer Acceleration.

Vous pouvez configurer Transfer Acceleration sur les compartiments nouveaux ou existants. Vous pouvez utiliser un point de terminaison Amazon S3 Transfer Acceleration distinct pour utiliser les emplacements AWS périphériques. Le meilleur moyen de tester si Transfer Acceleration améliore les performances des demandes des clients consiste à utiliser l'Outil de comparaison de la vitesse de Amazon S3 Transfer Acceleration. Les configurations et les états du réseau varient de temps à autre et d'emplacement à emplacement. Par conséquent, vous n'êtes facturé que pour les transferts où

Amazon S3 Transfer Acceleration peut potentiellement améliorer vos performances de chargement. Pour plus d'informations sur l'utilisation de Transfer Acceleration avec différents types AWS SDKs, consultezActivation et utilisation de S3 Transfer Acceleration.

Hébergement d'un site Web statique à l'aide d'Amazon S3

Vous pouvez utiliser Amazon S3 pour héberger un site web statique. Sur un site web statique, les pages web individuelles contiennent du contenu statique. Elles peuvent également contenir des scénarios côté client.

> **Note**
>
> Nous vous recommandons AWS Amplify d'utiliser l'hébergement pour héberger le contenu statique d'un site Web stocké sur S3. Amplify Hosting est un service entièrement géré qui facilite le déploiement de vos sites Web sur un réseau de diffusion de contenu (CDN) disponible dans le monde entier alimenté par Amazon CloudFront, permettant ainsi un hébergement de sites Web statique sécurisé.
> Avec AWS Amplify Hosting, vous pouvez sélectionner l'emplacement de vos objets dans votre compartiment à usage général, déployer votre contenu sur un CDN géré et générer une URL HTTPS publique pour que votre site Web soit accessible partout. Pour plus d'informations sur l'hébergement Amplify, consultez Déploiement d'un site Web statique vers un AWS Amplify hébergement à partir d'un compartiment à usage général S3 et Déploiement d'un site Web statique depuis S3 à l'aide de la console Amplify dans le guide de l'utilisateur de la AWS Amplify console.

Pour plus d'informations sur l'hébergement d'un site Web statique sur Amazon S3, y compris les instructions et les step-by-step procédures pas à pas, consultez les rubriques suivantes.

Rubriques

- Points de terminaison de sites web
- Activation de l'hébergement de sites web
- Configuration d'un document d'index
- Configuration d'un document d'erreur personnalisé
- Définition des autorisations pour l'accès au site web
- (Facultatif) Journalisation du trafic web
- (Facultatif) Configuration de la redirection de pages web
- Utilisation du partage des ressources entre origines multiples (CORS)

- Didacticiels relatifs aux sites Web statiques

Points de terminaison de sites web

Lorsque vous configurez votre compartiment en tant que site web statique, il est disponible au point de terminaison du site web spécifique de la Région AWS du compartiment. Les points de terminaison de sites Web sont différents de ceux auxquels vous adressez des demandes d'API REST. Pour plus d'informations sur les différences entre les points de terminaison, consultez Différences clés entre un point de terminaison de site web et un point de terminaison de l'API REST.

En fonction de votre Région, le point de terminaison de votre site web Amazon S3 respecte l'un des deux formats suivants.

- s3-siteweb tiret (-) Région - `http://bucket-name.s3-website-Region.amazonaws.com`
- s3-siteweb point (.) Région - `http://bucket-name.s3-website.Region.amazonaws.com`

Ils URLs renvoient le document d'index par défaut que vous configurez pour le site Web. Pour obtenir la liste complète des points de terminaison de sites Web Amazon S3, consultez Points de terminaison de sites Web Amazon S3.

> **Note**
>
> Pour renforcer la sécurité de vos sites Web statiques Amazon S3, les domaines de point de terminaison des sites Web Amazon S3 (par exemple, s3- website-us-east -1.amazonaws.com ou s3-website.ap-south-1.amazonaws.com) sont enregistrés dans la liste des suffixes publics (PSL). Pour plus de sécurité, nous vous recommandons d'utiliser des cookies avec un préfixe `__Host-` si vous devez définir des cookies sensibles dans le nom de domaine de vos sites web statiques Amazon S3. Cette pratique vous aidera à protéger votre domaine contre les tentatives de falsification de requêtes intersites (CSRF). Pour plus d'informations, consultez la page Set-Cookie du Mozilla Developer Network.

Si vous souhaitez que votre site web soit public, vous devez rendre l'ensemble de votre contenu accessible publiquement en lecture pour que vos clients puissent accéder au point de terminaison du site web. Pour plus d'informations, consultez Définition des autorisations pour l'accès au site web.

Important

- Les points de terminaison de site web Amazon S3 ne prennent pas en charge le protocole HTTPS ou les points d'accès. Si vous souhaitez utiliser le protocole HTTPS, vous pouvez effectuer l'une des opérations suivantes :
  - (Recommandé) Utilisez l'AWS Amplify hébergement pour héberger le contenu statique d'un site Web stocké sur S3. Amplify Hosting est un service entièrement géré qui facilite le déploiement de vos sites Web sur un réseau de diffusion de contenu (CDN) disponible dans le monde entier alimenté par Amazon CloudFront, permettant ainsi un hébergement de sites Web statique sécurisé.

    Avec AWS Amplify Hosting, vous pouvez sélectionner l'emplacement de vos objets dans votre compartiment à usage général, déployer votre contenu sur un CDN géré et générer une URL HTTPS publique pour que votre site Web soit accessible partout. Pour plus d'informations sur l'hébergement Amplify, consultez Déploiement d'un site Web statique vers un AWS Amplify hébergement à partir d'un compartiment à usage général S3 et Déploiement d'un site Web statique depuis S3 à l'aide de la console Amplify dans le guide de l'utilisateur de la AWS Amplify console.
  - Utilisez Amazon CloudFront pour proposer un site Web statique hébergé sur Amazon S3. Pour plus d'informations, consultez Comment utiliser CloudFront pour répondre aux requêtes HTTPS pour mon compartiment Amazon S3 ? Pour utiliser le protocole HTTPS avec un domaine personnalisé, consultez Configuration d'un site web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53.
- Les compartiments de type Paiement par le demandeur ne permettent pas l'accès via un point de terminaison de site web. Toute demande à un compartiment de type reçoit une réponse 403 Accès refusé. Pour plus d'informations, consultez Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation.

Rubriques

- Exemples de point de terminaison de site web
- Ajout d'un DNS CNAME
- Utilisation d'un domaine personnalisé avec Route 53

- Différences clés entre un point de terminaison de site web et un point de terminaison de l'API REST

Exemples de point de terminaison de site web

Les exemples suivants montrent comment accéder à un compartiment Amazon S3 configuré en tant que site web statique.

Example - Demande d'un objet au niveau racine

Pour demander un objet spécifique stocké au niveau racine dans le compartiment, utilisez la structure d'URL suivante.

```
http://bucket-name.s3-website.Region.amazonaws.com/object-name
```

Par exemple, l'URL suivante demande l'objet `photo.jpg` stocké au niveau racine dans le compartiment.

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/photo.jpg
```

Example - Demande d'un objet dans un préfixe

Pour demander un objet stocké dans un dossier de votre compartiment, utilisez la structure d'URL suivante.

```
http://bucket-name.s3-website.Region.amazonaws.com/folder-name/object-name
```

L'URL suivante demande l'objet `docs/doc1.html` dans votre compartiment.

```
http://example-bucket.s3-website.us-west-2.amazonaws.com/docs/doc1.html
```

Ajout d'un DNS CNAME

Si vous avez un domaine enregistré, vous pouvez ajouter une entrée DNS CNAME pour diriger vers le point de terminaison du site Web Amazon S3. A titre d'exemple, si vous avez enregistré le domaine `www.example-bucket.com`, vous pouvez créer un compartiment `www.example-bucket.com` et ajouter un enregistrement DNS CNAME qui pointe vers `www.example-bucket.com.s3-website.Region.amazonaws.com`. Toutes les demandes adressées à

`http://www.example-bucket.com` sont réacheminées vers `www.example-bucket.com.s3-website.Region.amazonaws.com`.

Pour plus d'informations, consultez Personnalisation d'Amazon S3 URLs avec des enregistrements CNAME.

Utilisation d'un domaine personnalisé avec Route 53

Au lieu d'accéder au site web à l'aide d'un point de terminaison de site web Amazon S3, vous pouvez utiliser votre propre domaine enregistré auprès d'Amazon Route 53 pour diffuser votre contenu (par exemple, `example.com`. Vous pouvez utiliser Amazon S3 avec Route 53 pour héberger un site web sur le domaine racine. À titre d'exemple, si votre domaine racine est `example.com` et que votre site web est hébergé sur Amazon S3, les visiteurs peuvent accéder à votre site web à partir de leur navigateur en entrant `http://www.example.com` ou `http://example.com`.

Pour afficher un exemple de procédure, consultez Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53.

Différences clés entre un point de terminaison de site web et un point de terminaison de l'API REST

Un point de terminaison de site web Amazon S3 est optimisé pour un accès depuis un navigateur web. Le tableau suivant résume les principales différences entre un point de terminaison de l'API REST et un point de terminaison de site web.

Principales différences	point de terminaison de l'API REST	point de terminaison des sites Web
Contrôle d'accès	Prend en charge les contenus public et privé	Prend en charge uniquement le contenu public
Gestion des messages d'erreur	Renvoie une réponse au format XML	Renvoie un document HTML
Prise en charge de redirection	Ne s'applique pas	Prend en charge les redirections au niveau de l'objet et du compartiment

Principales différences	point de terminaison de l'API REST	point de terminaison des sites Web
Demandes prises en charge	Prend en charge les opérations relatives aux compartiments et aux objets.	Supports uniquement `GET` et `HEAD` demandes portant sur des objets
Réponses `GET` et `HEAD` demandes à la racine d'un bucket	Renvoie une liste de clés d'objet dans le compartiment	Renvoie le document d'index qui est spécifié dans la configuration du site Web
Prise en charge du protocole SSL (Secure Sockets Layer)	Prend en charge toutes les connexions SSL	Ne prend pas en charge les connexions SSL

Pour obtenir la liste complète des points de terminaison Amazon S3, consultez Points de terminaison et quotas Amazon S3 dans la Références générales AWS.

Activation de l'hébergement de sites web

Lorsque vous configurez un compartiment en tant que site Web statique, vous devez activer l'hébergement de sites Web statiques, configurer un document d'index et définir des autorisations.

Vous pouvez activer l'hébergement statique de sites Web à l'aide de la console Amazon S3, de l'API REST AWS SDKs AWS CLI, du ou AWS CloudFormation.

Pour configurer votre site Web avec un domaine personnalisé, consultez Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53.

Utiliser la console S3.

Pour activer l'hébergement de site Web statique

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.

3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer l'hébergement statique de sites Web.
4. Choisissez Propriétés.
5. Sous Static website hosting (Hébergement de site Web statique), choisissez Edit (Modifier).
6. Choisissez Utiliser ce compartiment pour héberger un site Web.
7. Sous Static website hosting (Hébergement de site web statique), choisissez Enable (Activer).
8. Dans Index document (Document d'index), entrez le nom du document d'index, généralement `index.html`.

   Le nom du document d'index est sensible à la casse et doit correspondre exactement au nom de fichier du document d'index HTML que vous prévoyez de charger dans votre compartiment S3. Lorsque vous configurez un compartiment pour l'hébergement d'un site web, vous devez indiquer un document d'index. Amazon S3 renvoie ce document d'index lorsque des demandes sont faites dans le domaine racine ou dans n'importe quel sous-dossier. Pour plus d'informations, consultez Configuration d'un document d'index.
9. Pour fournir votre propre document d'erreur personnalisé pour les erreurs de classe 4XX, entrez le nom du fichier du document d'erreur personnalisé dans Document d'erreur.

   Le nom du document d'erreur est sensible à la casse et doit correspondre exactement au nom de fichier du document d'erreur HTML que vous prévoyez de charger dans votre compartiment S3. Si vous ne spécifiez pas de document d'erreur personnalisé et qu'une erreur se produit, Amazon S3 renvoie un document d'erreur HTML par défaut. Pour plus d'informations, consultez Configuration d'un document d'erreur personnalisé.
10. (Facultatif) Si vous souhaitez spécifier des règles de redirection avancées, décrivez les règles à l'aide du langage JSON dans Redirection rules (Règles de redirection).

    Par exemple, vous pouvez acheminer les demandes de façon conditionnelle en fonction des noms ou préfixes de clés d'objets dans la demande. Pour plus d'informations, consultez Configurer des règles de redirection pour utiliser des redirections conditionnelles avancées.
11. Choisissez Enregistrer les modifications.

    Amazon S3 permet l'hébergement de site web statique pour votre compartiment. Au bas de la page, sous Static website hosting (Hébergement de site Web statique), vous voyez le point de terminaison du site web pour votre compartiment.
12. Sous Static website hosting (Hébergement de site Web statique), notez la valeur de Endpoint (Point de terminaison).

Endpoint (Point de terminaison) correspond au point de terminaison du site web Amazon S3 de votre compartiment. Une fois que vous avez terminé de configurer votre compartiment en tant que site Web statique, vous pouvez utiliser ce point de terminaison pour tester votre site Web.

Utilisation de l'API REST

Pour plus d'informations sur l'envoi direct de demandes REST afin d'activer l'hébergement de site Web statique, consultez les sections suivantes dans le manuel Référence d'API Amazon Simple Storage Service :

- PUT Bucket website
- GET Bucket website
- DELETE Bucket website

En utilisant le AWS SDKs

Pour héberger un site web statique dans Amazon S3, vous configurez un compartiment Amazon S3 pour l'hébergement de site web, puis vous chargez le contenu du site web dans le compartiment. Vous pouvez également utiliser le AWS SDKs pour créer, mettre à jour et supprimer la configuration du site Web par programmation. Ils SDKs fournissent des classes wrapper autour de l'API REST Amazon S3. Vous pouvez envoyer des demandes d'API REST directement à partir de l'application, si cette dernière l'exige.

.NET

L'exemple suivant montre comment utiliser le AWS SDK pour .NET pour gérer la configuration du site Web d'un bucket. Pour ajouter une configuration de site Web à un compartiment, vous fournissez un nom de compartiment et une configuration de site Web. La configuration de site Web doit comprendre un document d'index et peut contenir un rapport d'erreur facultatif. Ces documents doivent être stockés dans le compartiment. Pour plus d'informations, consultez PUT Bucket website. Pour plus d'informations sur la fonctionnalité du site Web Amazon S3, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.

L'exemple de code C# suivant ajoute une configuration de site Web sur le compartiment spécifié. La configuration spécifie les noms du document d'index et du rapport d'erreur. Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class WebsiteConfigTest
    {
        private const string bucketName = "*** bucket name ***";
        private const string indexDocumentSuffix = "*** index object key ***"; //
 For example, index.html.
        private const string errorDocument = "*** error object key ***"; // For
 example, error.html.
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 client;
        public static void Main()
        {
            client = new AmazonS3Client(bucketRegion);
            AddWebsiteConfigurationAsync(bucketName, indexDocumentSuffix,
 errorDocument).Wait();
        }

        static async Task AddWebsiteConfigurationAsync(string bucketName,
                                            string indexDocumentSuffix,
                                            string errorDocument)
        {
            try
            {
                // 1. Put the website configuration.
                PutBucketWebsiteRequest putRequest = new PutBucketWebsiteRequest()
                {
                    BucketName = bucketName,
                    WebsiteConfiguration = new WebsiteConfiguration()
                    {
                        IndexDocumentSuffix = indexDocumentSuffix,
                        ErrorDocument = errorDocument
                    }
                };
```

```
                PutBucketWebsiteResponse response = await
 client.PutBucketWebsiteAsync(putRequest);

                // 2. Get the website configuration.
                GetBucketWebsiteRequest getRequest = new GetBucketWebsiteRequest()
                {
                    BucketName = bucketName
                };
                GetBucketWebsiteResponse getResponse = await
 client.GetBucketWebsiteAsync(getRequest);
                Console.WriteLine("Index document: {0}",
 getResponse.WebsiteConfiguration.IndexDocumentSuffix);
                Console.WriteLine("Error document: {0}",
 getResponse.WebsiteConfiguration.ErrorDocument);
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
 writing an object", e.Message);
            }
        }
    }
}
```

PHP

L'exemple PHP suivant ajoute une configuration de site Web au compartiment spécifié. La méthode `create_website_config` fournit explicitement les noms du document d'index et du rapport d'erreur. L'exemple récupère également la configuration de site Web et affiche la réponse. Pour plus d'informations sur la fonctionnalité du site Web Amazon S3, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.

Pour plus d'informations sur l'API AWS SDK for Ruby, consultez AWS SDK for Ruby - Version 2.

```
 require 'vendor/autoload.php';

use Aws\S3\S3Client;
```

```
$bucket = '*** Your Bucket Name ***';

$s3 = new S3Client([
    'version' => 'latest',
    'region'  => 'us-east-1'
]);


// Add the website configuration.
$s3->putBucketWebsite([
    'Bucket'                => $bucket,
    'WebsiteConfiguration'  => [
        'IndexDocument' => ['Suffix' => 'index.html'],
        'ErrorDocument' => ['Key' => 'error.html']
    ]
]);

// Retrieve the website configuration.
$result = $s3->getBucketWebsite([
    'Bucket' => $bucket
]);
echo $result->getPath('IndexDocument/Suffix');

// Delete the website configuration.
$s3->deleteBucketWebsite([
    'Bucket' => $bucket
]);
```

En utilisant le AWS CLI

Pour plus d'informations sur l'utilisation du AWS CLI pour configurer un compartiment S3 en tant que site Web statique, consultez le site Web dans le manuel de référence des AWS CLI commandes.

Ensuite, vous devez configurer le document d'index et définir les autorisations. Pour plus d'informations, consultez Configuration d'un document d'index et Définition des autorisations pour l'accès au site web.

Vous pouvez également configurer un document d'erreur, la journalisation du trafic web ou une redirection.

Configuration d'un document d'index

Lorsque vous activez l'hébergement de site web, vous devez également configurer et charger un document d'index. Un document d'index est une page web renvoyée par Amazon S3 quand une demande est effectuée au niveau de la racine d'un site web ou de n'importe quel sous-dossier. A titre d'exemple, si un utilisateur entre `http://www.example.com` dans le navigateur, l'utilisateur ne demande pas de page spécifique. Dans ce cas, Amazon S3 affiche le document d'index, qui est parfois appelé page par défaut.

Lorsque vous activez l'hébergement de site web statique pour votre compartiment, vous saisissez le nom du document d'index (par exemple, `index.html`). Après avoir activé l'hébergement de site web statique pour votre compartiment, vous chargez un fichier HTML avec le nom du document d'index dans votre compartiment.

La barre oblique à la fin de l'URL racine est facultative. Par exemple, si vous configurez votre site Web `index.html` comme document d'index, l'une des valeurs suivantes URLs renvoie le résultat`index.html`.

```
http://example-bucket.s3-website.Region.amazonaws.com/
http://example-bucket.s3-website.Region.amazonaws.com
```

Pour plus d'informations sur les points de terminaison des sites web Amazon S3, consultez Points de terminaison de sites web.

Document d'index et dossiers

Dans Amazon S3, un compartiment est un conteneur plat d'objets. Il ne fournit pas une structure hiérarchique contrairement au système de fichiers sur votre ordinateur. Cependant, vous pouvez créer une hiérarchie logique à l'aide des noms de clés d'objet qui nécessitent une structure de dossiers.

Imaginons, par exemple, un compartiment avec trois objets et les noms de clés suivants : Bien qu'ils soient stockés sans structure hiérarchique physique, vous pouvez deviner l'arborescence logique des dossiers à partir des noms de clés :

- `sample1.jpg` - L'objet est situé à la racine du compartiment.
- `photos/2006/Jan/sample2.jpg` - L'objet est situé dans le sous-dossier `photos/2006/Jan`.
- `photos/2006/Feb/sample3.jpg` - L'objet est situé dans le sous-dossier `photos/2006/Feb`.

Dans la console Amazon S3, vous pouvez également créer un dossier dans un compartiment. Par exemple, vous pouvez créer un dossier nommé `photos`. Vous pouvez charger des objets dans le compartiment ou dans le dossier `photos` du compartiment. Si vous ajoutez l'objet `sample.jpg` dans le compartiment, le nom de la clé est `sample.jpg`. Si vous chargez l'objet dans le dossier `photos`, le nom de la clé d'objet est `photos/sample.jpg`.

Si vous créez une structure de dossiers dans votre compartiment, vous devez avoir un document d'index à chaque niveau. Le document d'index doit avoir le même nom dans chaque dossier, par exemple, `index.html`. Lorsqu'un utilisateur spécifie une URL qui se présente comme une recherche de répertoire, la présence ou l'absence d'une barre oblique finale détermine le comportement du site Web. A titre d'exemple, l'URL suivante, avec une barre oblique finale, renvoie le document d'index `photos/index.html`.

```
http://bucket-name.s3-website.Region.amazonaws.com/photos/
```

Néanmoins, si vous supprimez la barre oblique finale dans la précédente URL, Amazon S3 recherche d'abord un objet `photos` dans le compartiment. Si l'objet `photos` est introuvable, il cherche alors un document d'index, `photos/index.html`. Si ce document est trouvé, Amazon S3 renvoie un message `302 Found` et pointe vers la clé `photos/`. Pour les demandes suivantes vers `photos/`, Amazon S3 renvoie `photos/index.html`. Si le document d'index est introuvable, Amazon S3 renvoie une erreur.

Configurer un document d'index

Pour configurer un document d'index à l'aide de la console S3, procédez comme suit. Vous pouvez également configurer un document d'index à l'aide de l'API REST AWS SDKs, du AWS CLI, du ou AWS CloudFormation.

> **Note**
>
> Dans un compartiment activé pour la gestion des versions, vous pouvez charger plusieurs copies de `index.html`, mais seule la version la plus récente est traitée. Pour plus d'informations sur la gestion des versions S3, consultez Conservation de plusieurs versions d'objets grâce à la gestion des versions S3.

Lorsque vous activez l'hébergement de site web statique pour votre compartiment, vous saisissez le nom du document d'index (par exemple, **`index.html`**). Après avoir activé l'hébergement de site web

statique pour le compartiment, vous téléchargez un fichier HTML avec le nom du document de cet index dans votre compartiment.

Pour configurer le document d'index

1. Créez un fichier `index.html`.

   Si vous n'avez pas de ficher `index.html`, vous pouvez utiliser le code HTML suivant pour en créer un :

   ```
   <html xmlns="http://www.w3.org/1999/xhtml" >
   <head>
       <title>My Website Home Page</title>
   </head>
   <body>
     <h1>Welcome to my website</h1>
     <p>Now hosted on Amazon S3!</p>
   </body>
   </html>
   ```

2. Enregistrez le fichier d'index au niveau local.

   Le nom du fichier du document d'index doit correspondre exactement au nom du document d'index que vous saisissez dans la boîte de dialogue Hébergement de site Web statique. Le nom du document d'index est sensible à la casse. Par exemple, si vous saisissez `index.html` pour le nom du Document d'index dans la boîte de dialogue Hébergement de site Web statique, le nom du fichier de votre document d'index doit également être `index.html` et non `Index.html`.

3. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

4. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.

5. Dans la liste des buckets, choisissez le nom du bucket que vous souhaitez utiliser pour héberger un site Web statique.

6. Activez l'hébergement de site Web statique pour votre compartiment et saisissez le nom exact de votre document d'index (par exemple, `index.html`). Pour plus d'informations, consultez Activation de l'hébergement de sites web.

   Après l'activation de l'hébergement de site web statique, passez à l'étape 6.

7. Pour charger le document d'index dans votre compartiment, effectuez l'une des opérations suivantes :

- Faites glisser et déposez le fichier d'index dans la liste du compartiment de la console.
- Choisissez Charger, puis suivez les instructions pour choisir et charger le fichier d'index.

Pour step-by-step obtenir des instructions, voirChargement d'objets.

8. (Facultatif) Chargez du contenus d'un autre site Web dans votre compartiment.

Ensuite, vous devez définir des autorisations pour l'accès au site web. Pour plus d'informations, consultez Définition des autorisations pour l'accès au site web.

Vous pouvez également configurer un document d'erreur, la journalisation du trafic web ou une redirection.

Configuration d'un document d'erreur personnalisé

Une fois que vous avez configuré votre compartiment en tant que site web statique, lorsqu'une erreur se produit, Amazon S3 renvoie un document d'erreur HTML. Vous pouvez éventuellement configurer votre compartiment avec un document d'erreur personnalisé afin que Amazon S3 renvoie ce document en cas d'erreur.

> **Note**
>
> Certains navigateurs affichent leur propre message d'erreur lorsqu'une erreur se produit, sans tenir compte du document d'erreur renvoyé par Amazon S3. A titre d'exemple, lorsqu'une erreur HTTP 404 Not Found se produit, Google Chrome peut afficher son propre message d'erreur, sans tenir compte du document d'erreur renvoyé par Amazon S3.

Rubriques

- Codes de réponse HTTP Amazon S3
- Configuration d'un document d'erreur personnalisé

Codes de réponse HTTP Amazon S3

Le tableau suivant répertorie le sous-ensemble des codes de réponse HTTP qu'Amazon S3 renvoie quand une erreur se produit.

Code d'erreur HTTP	Description
301 – Déplacé de façon permanente	Lorsqu'un utilisateur envoie une demande directement au point de terminaison du site web Amazon S3 (`http://s3-website.` *`Region`*`.amazonaws.com/`), Amazon S3 renvoie une réponse 301 Moved Permanently (Déplacé de façon permanente) et redirige ces demandes vers `https://aws.amazon.com/s3/` .
302 – Trouvé	Quand Amazon S3 reçoit une demande pour une clé `x`, `http://`*`bucket-name`*`.s3-website.`*`Region`*`.amazonaws.com/x` , sans barre oblique finale, il recherche d'abord l'objet portant le nom de clé `x`. Si l'objet est introuvable, Amazon S3 en conclut que la demande concerne le sous-dossier `x` et redirige la demande en ajoutant une barre oblique à la fin, puis renvoie le code 302 Found (Trouvé).
304 – Non modifié	Amazon S3 utilise des en-têtes de requête `If-Modified-Since` , `If-Unmodified-Since` , `If-Match` et/ou `If-None-Match` pour déterminer si l'objet demandé est identique à la copie mise en cache conservée par le client. Si l'objet est le même, le point de terminaison de site web renvoie une réponse 304 – Non modifié.
400 – Demande incorrecte	Le point de terminaison de site web renvoie un code 400 – Demande incorrecte quand l'utilisateur tente d'accéder à un compartiment via le point de terminaison Régional incorrect.
403 Forbidden	Le point de terminaison de site web renvoie le code d'erreur 403 Forbidden quand la demande de l'utilisateur est traduite en objet qui n'est pas accessible en lecture au public. Le propriétaire de l'objet doit permettre l'accès à l'objet en lecture au public via la politique de compartiment ou une liste ACL.
404 – Non trouvé	Le point de terminaison de site web renvoie le code d'erreur 404 – Non trouvé pour les raisons suivantes : •

Code d'erreur HTTP	Description
	Amazon S3 identifie que l'URL du site web fait référence à une clé d'objet qui n'existe pas. • Amazon S3 en déduit que la demande concerne un document d'index qui n'existe pas. • Le compartiment spécifié dans l'URL n'existe pas. • Le compartiment spécifié dans l'URL existe, mais n'est pas configuré comme un site web. Vous pouvez créer un document personnalisé qui sera renvoyé dans le cadre du code 404 – Non trouvé. Assurez-vous que le document est chargé dans le compartiment configuré comme un site web et que la configuration d'hébergement du site web est définie pour utiliser le document. Pour plus d'informations sur la façon dont Amazon S3 interprète l'URL comme une demande pour un objet ou un document d'index, consultez Configuration d'un document d'index.
500 – Erreur service	Le point de terminaison de site web répond avec le code 500 – Erreur service quand une erreur interne du serveur se produit.
503 – Service non disponible	Le point de terminaison du site web répond avec le code 503 Service Unavailable (Service non disponible) quand Amazon S3 détermine que vous devez réduire le débit des demandes.

Pour chacune de ces erreurs, Amazon S3 renvoie un message HTML prédéfini. Voici un exemple de message HTML renvoyé pour une réponse 403 Forbidden.



Configuration d'un document d'erreur personnalisé

Lorsque vous configurez votre compartiment en tant que site Web statique, vous pouvez fournir un document d'erreur personnalisé contenant un message d'erreur explicite et des conseils supplémentaires. Amazon S3 renvoie votre document d'erreur personnalisé uniquement pour la classe HTTP 4xx des codes d'erreur.

Pour configurer un document d'erreur personnalisé à l'aide de la console S3, procédez comme suit. Vous pouvez également configurer un document d'erreur à l'aide de l'API REST AWS SDKs, du AWS CLI, du ou AWS CloudFormation. Pour plus d'informations, consultez les ressources suivantes :

- PutBucketWebsitedans le manuel de référence de l'API Amazon Simple Storage Service
- AWS::S3::Bucket WebsiteConfiguration dans le guide de l'utilisateur AWS CloudFormation
- put-bucket-website dans la référence de commande de l'AWS CLI

Lorsque vous activez l'hébergement de site Web statique pour votre compartiment, vous entrez le nom du document d'erreur (par exemple, **`404.html`**). Après avoir activé l'hébergement de site web statique pour le compartiment, vous chargez un fichier HTML avec le nom du document d'erreur dans votre compartiment.

Pour configurer un document d'erreur

1. Créez un document d'erreur, par exemple `404.html`.
2. Enregistrez le fichier de document d'erreur au niveau local.

Le nom du document d'erreur est sensible à la casse et doit correspondre exactement au nom que vous saisissez lorsque vous activez l'hébergement de site web statique. Par exemple, si vous entrez `404.html` pour le nom du document d'Erreur dans la boîte de dialogue Hébergement de site Web statique, le nom de fichier de votre document d'erreur doit également être `404.html`.

3. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
4. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
5. Dans la liste des buckets, choisissez le nom du bucket que vous souhaitez utiliser pour héberger un site Web statique.
6. Activez l'hébergement de site Web statique pour votre compartiment et entrez le nom exact de votre document d'erreur (par exemple, `404.html`). Pour plus d'informations, consultez Activation de l'hébergement de sites web et Configuration d'un document d'erreur personnalisé.

   Après l'activation de l'hébergement de site web statique, passez à l'étape 6.
7. Pour charger le document d'erreur dans votre compartiment, effectuez l'une des opérations suivantes :

   - Faites glisser et déposez le fichier du document d'erreur dans la liste des compartiments de la console.
   - Choisissez Upload (Charger), puis suivez les instructions pour choisir et charger le fichier d'index.

   Pour step-by-step obtenir des instructions, voirChargement d'objets.

Définition des autorisations pour l'accès au site web

Lorsque vous configurez un compartiment en tant que site web statique, si vous voulez que votre site web soit public, vous pouvez accorder un accès public en lecture. Pour que votre compartiment soit lisible publiquement, vous devez désactiver les paramètres de blocage de l'accès public pour le compartiment et écrire une politique de compartiment qui octroie un accès en lecture public. Si votre compartiment contient des objets qui n'appartiennent pas au propriétaire du compartiment, il se peut que vous ayez également besoin d'ajouter une liste ACL des objets qui accorde l'accès en lecture à tous.

Si vous ne souhaitez pas désactiver les paramètres de blocage de l'accès public pour votre compartiment, mais que vous souhaitez tout de même que votre site Web soit public, vous pouvez créer une CloudFront distribution Amazon pour servir votre site Web statique. Pour plus d'informations, consultez Accélérez votre site Web avec Amazon CloudFront ou utilisez une CloudFront distribution Amazon pour servir un site Web statique dans le guide du développeur Amazon Route 53.

> **Note**
>
> Sur le point de terminaison du site web, si un utilisateur demande un objet qui n'existe pas, Amazon S3 renvoie le code réponse HTTP `404 (Not Found)`. Si l'objet existe, mais que vous n'avez pas l'autorisation en lecture dessus, le point de terminaison du site Web renvoie un code réponse HTTP `403 (Access Denied)`. L'utilisateur peut utiliser le code réponse pour déduire si un objet spécifique existe ou non. Si vous ne voulez pas ce type de comportement, vous ne devez pas activer la prise en charge du site Web pour votre compartiment.

Rubriques

- Étape 1 : modifier les paramètres de blocage de l'accès public S3
- Étape 2 : ajouter une politique de compartiment
- Listes de contrôle d'accès à l'objet

Étape 1 : modifier les paramètres de blocage de l'accès public S3

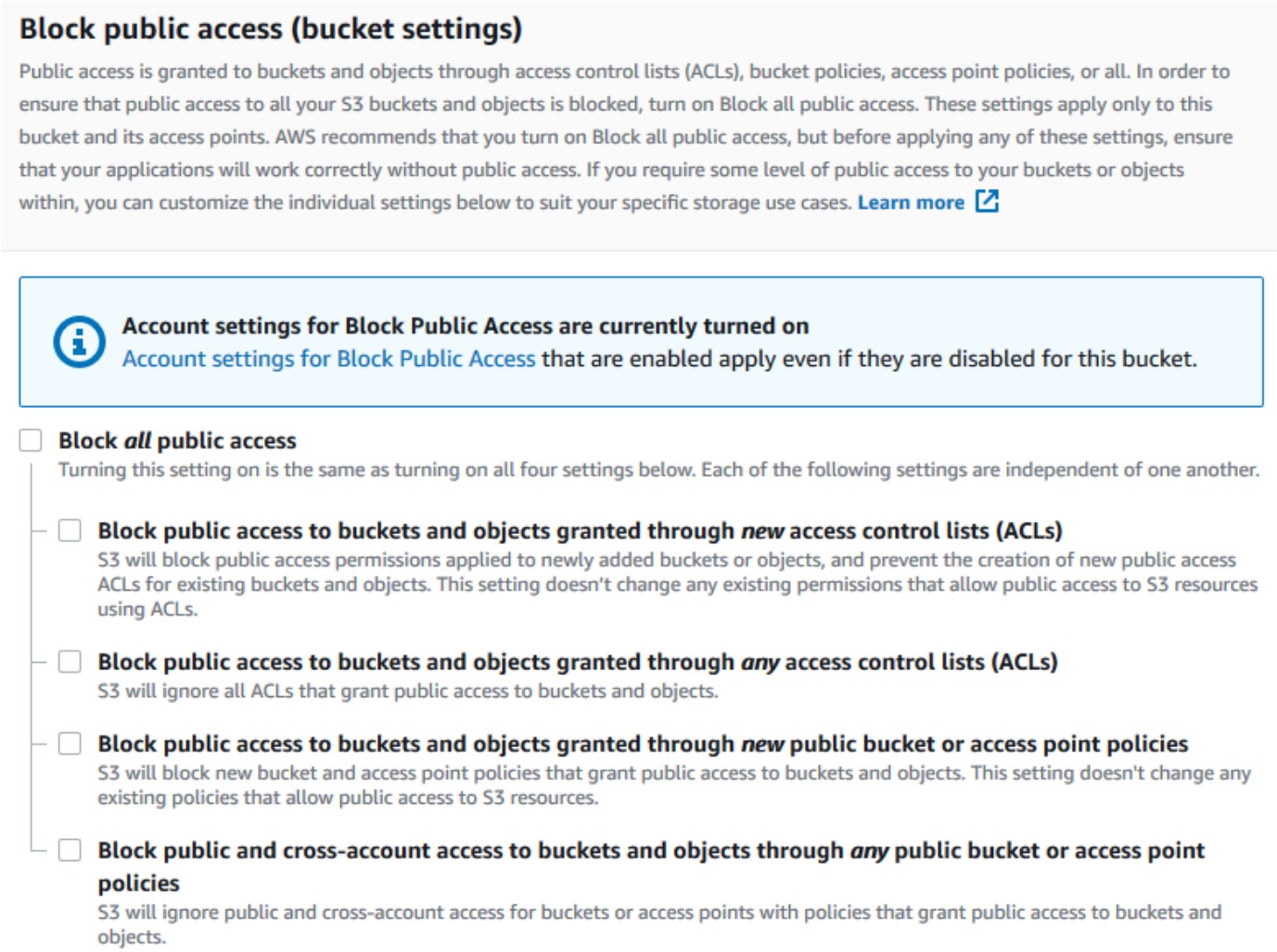
Si vous voulez configurer un compartiment existant en tant que site web statique ayant un accès public, vous devez modifier les paramètres de blocage de l'accès public pour ce compartiment. Vous devrez peut-être également modifier les paramètres de blocage de l'accès public au niveau de votre compte. Amazon S3 applique la combinaison la plus restrictive de paramètres de blocage de l'accès public au niveau du compartiment et du compte.

Par exemple, si vous autorisez l'accès public pour un compartiment, mais que vous bloquez tout accès public au niveau du compte, Amazon S3 continue de bloquer l'accès public au compartiment. Dans ce scénario, vous devez modifier vos paramètres de blocage de l'accès public de niveau compartiment et de niveau compte. Pour plus d'informations, consultez Blocage de l'accès public à votre stockage Amazon S3.

Par défaut, Amazon S3 bloque l'accès public à votre compte et à vos compartiments. Si vous souhaitez utiliser un compartiment pour héberger un site web statique, vous pouvez utiliser ces étapes pour modifier vos paramètres de blocage de l'accès public.

> **Warning**
>
> Avant de suivre ces étapes, passez en revue Blocage de l'accès public à votre stockage Amazon S3 pour vous assurer que vous comprenez et acceptez les risques liés à l'autorisation de l'accès public. Lorsque vous désactivez les paramètres de blocage de l'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tous les accès publics à vos compartiments.

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le nom du compartiment que vous avez configuré en tant que site web statique.
3. Choisissez Permissions.
4. Sous Block public access (bucket settings) (Bloquer l'accès public (paramètres de compartiment)), choisissez Edit (Modifier).
5. Décochez Bloquer tous les accès publics et sélectionnez Enregistrer les modifications.



Amazon S3 désactive les paramètres de blocage de l'accès public pour votre compartiment. Pour créer un site Web public statique, vous devrez peut-être aussi modifier les paramètres de blocage de l'accès public de votre compte avant d'ajouter une politique de compartiment. Si les paramètres de blocage de l'accès public pour votre compte sont actuellement activés, une note s'affiche sous Bloquer l'accès public (paramètres de compartiment).

Étape 2 : ajouter une politique de compartiment

Pour que les objets de votre compartiment soient publiquement lisibles, vous devez écrire une politique de compartiment qui accorde à tous l'autorisation `s3:GetObject`.

Après avoir modifié les paramètres de blocage de l'accès public S3, vous devez ajouter une politique de compartiment pour accorder un accès public en lecture à votre compartiment. Lorsque vous accordez un accès public en lecture, tout le monde sur Internet peut accéder à votre compartiment.

> **Important**
>
> La stratégie suivante est uniquement un exemple et autorise un accès complet au contenu de votre compartiment. Avant d'effectuer cette étape, consultez Comment assurer la sécurité des fichiers de mon compartiment Amazon S3 ?, pour vous assurer que vous comprenez les bonnes pratiques pour sécuriser les fichiers dans votre compartiment S3 et les risques liés à l'octroi d'un accès public.

1. Dans Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Permissions.
3. Sous Politique de compartiment, choisissez Modifier.
4. Pour accorder l'accès public en lecture à votre site web, copiez la politique de compartiment suivante et collez-la dans l'Éditeur de politique de compartiment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. Mettez à jour `Resource` pour inclure le nom de votre compartiment.

   Dans l'exemple de politique de compartiment précédent, *`Bucket-Name`* il s'agit d'un espace réservé pour le nom du compartiment. Pour utiliser cette politique de compartiment avec votre propre compartiment, vous devez mettre à jour ce nom pour qu'il corresponde à celui de votre compartiment.
6. Sélectionnez Enregistrer les modifications.

Un message s'affiche indiquant que la politique de compartiment a été ajoutée avec succès.

Si une erreur indique `Policy has invalid resource`, confirmez que le nom du compartiment dans la politique de compartiment correspond au nom de votre compartiment. Pour plus d'informations sur l'ajout d'une politique de compartiment, consultez Comment ajouter une politique de compartiment S3 ?

Si vous recevez un message d'erreur et que vous ne pouvez pas enregistrer la politique de compartiment, vérifiez les paramètres de blocage de l'accès public de votre compte et de votre compartiment pour confirmer que vous autorisez l'accès public au compartiment.

Listes de contrôle d'accès à l'objet

Vous pouvez utiliser une politique de compartiment pour accorder des autorisations à vos objets. Cependant, la politique de compartiment s'applique uniquement aux objets appartenant au propriétaire du compartiment. Si votre compartiment contient des objets qui n'appartiennent pas au propriétaire du compartiment, l'autorisation READ publique sur ces objets doit être accordée à l'aide de la liste ACL des objets.

La propriété des objets S3 est un paramètre au niveau du compartiment Amazon S3 que vous pouvez utiliser à la fois pour contrôler la propriété des objets chargés dans votre compartiment et pour les désactiver ou les activer. ACLs Par défaut, Object Ownership est défini sur le paramètre imposé par le propriétaire du bucket, et tous ACLs sont désactivés. Lorsqu'ils ACLs sont désactivés, le propriétaire du compartiment possède tous les objets du compartiment et gère l'accès à ceux-ci exclusivement à l'aide de politiques de gestion des accès.

La majorité des cas d'utilisation modernes d'Amazon S3 ne nécessitent plus l'utilisation de ACLs. Nous vous recommandons de rester ACLs désactivé, sauf dans des circonstances exceptionnelles où vous devez contrôler l'accès à chaque objet individuellement. Lorsque cette ACLs option est désactivée, vous pouvez utiliser des politiques pour contrôler l'accès à tous les objets de votre compartiment, quelle que soit la personne qui les a chargés dans votre compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

> **Important**
>
> Si votre compartiment à usage général utilise le paramètre imposé par le propriétaire du compartiment pour la propriété des objets S3, vous devez utiliser des politiques

pour accorder l'accès à votre compartiment à usage général et aux objets qu'il contient. Lorsque le paramètre Bucket owner forced est activé, les demandes de définition de listes de contrôle d'accès (ACLs) ou de mise à jour ACLs échouent et renvoient le code `AccessControlListNotSupported` d'erreur. Les demandes de lecture ACLs sont toujours prises en charge.

Pour qu'un objet soit accessible en lecture publiquement à l'aide d'une liste ACL, accordez une autorisation READ au groupe `AllUsers`, comme indiqué dans l'élément « grant » suivant. Ajoutez cet élément « grant » à la liste ACL d'objet. Pour plus d'informations sur la gestion ACLs, consultezPrésentation de la liste de contrôle d'accès (ACL).

```
<Grant>
  <Grantee xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:type="Group">
    <URI>http://acs.amazonaws.com/groups/global/AllUsers</URI>
  </Grantee>
  <Permission>READ</Permission>
</Grant>
```

(Facultatif) Journalisation du trafic web

Vous pouvez éventuellement activer la journalisation des accès au serveur Amazon S3 pour un compartiment configuré en tant que site web statique. La journalisation des accès au serveur fournit des enregistrements détaillés pour les demandes soumises à votre compartiment. Pour de plus amples informations, veuillez consulter Enregistrement de demandes avec journalisation des accès au serveur. Si vous envisagez d'utiliser Amazon CloudFront pour accélérer votre site Web, vous pouvez également utiliser la CloudFront journalisation. Pour plus d'informations, consultez la section Configuration et utilisation des journaux d'accès dans le manuel Amazon CloudFront Developer Guide.

Pour activer la journalisation des accès au serveur pour votre compartiment de site web statique

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la même région où vous avez créé le compartiment configuré en tant que site Web statique, créez un compartiment à usage général pour la journalisation, par exemple`logs.example.com`.
3. Créez un dossier pour les fichiers de journalisation des accès au serveur (par exemple, `logs`).

4. (Facultatif) Si vous souhaitez l'utiliser CloudFront pour améliorer les performances de votre site Web, créez un dossier pour les fichiers CloudFront journaux (par exemple,`cdn`).

   Pour de plus amples informations, veuillez consulter Accélérez votre site Web avec Amazon CloudFront.
5. Dans la liste Compartiments, choisissez le nom de votre compartiment.
6. Choisissez Propriétés.
7. Sous Server access logging (Journalisation des accès au serveur), choisissez Edit (Modifier).
8. Sélectionnez Activer.
9. Sous Target bucket (Compartiment cible), choisissez la destination du compartiment et du dossier pour les journaux d'accès au serveur :

   - Accédez à l'emplacement du dossier et du compartiment :
     1. Choisissez Parcourir S3.
     2. Choisissez le nom du compartiment, puis le dossier des journaux.
     3. Choisissez Choose path (Sélectionnez un chemin).
   - Saisissez le chemin du compartiment S3, par ex., **`s3://logs.example.com/logs/`**.
10. Choisissez Enregistrer les modifications.

    Dans votre compartiment de journaux, vous pouvez désormais accéder à vos journaux. Amazon S3 copie les journaux d'accès du site web dans votre compartiment de journaux toutes les deux heures.

(Facultatif) Configuration de la redirection de pages web

Si votre compartiment Amazon S3 est configuré pour l'hébergement de site web statique, vous pouvez configurer des redirections pour votre compartiment ou les objets qu'il contient. Vous disposez des options suivantes pour configurer des redirections.

Rubriques

- Rediriger les demandes pour le point de terminaison de site web de votre compartiment vers un autre compartiment ou domaine
- Configurer des règles de redirection pour utiliser des redirections conditionnelles avancées
- Rediriger les demandes pour un objet

Rediriger les demandes pour le point de terminaison de site web de votre compartiment vers un autre compartiment ou domaine

Vous pouvez rediriger toutes les demandes d'un point de terminaison de site web pour un compartiment vers un autre compartiment ou domaine. Si vous redirigez toutes les demandes, chaque demande adressée au point de terminaison de site web est redirigée vers le compartiment ou le domaine spécifié.

Par exemple, si votre domaine racine est `example.com`, et que vous souhaitez gérer des demandes pour `http://example.com` et `http://www.example.com`, vous devez créer deux compartiments nommés `example.com` et `www.example.com`. Ensuite, gérez le contenu dans le compartiment `example.com` et configurez l'autre compartiment `www.example.com` de manière à rediriger toutes les demandes vers le compartiment `example.com`. Pour plus d'informations, consultez les informations relatives à la configuration d'un site Web statique à l'aide d'un nom de domaine personnalisé.

Pour rediriger des demandes pour un point de terminaison de site Web de compartiment

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Sous Buckets (Compartiments), choisissez le nom du compartiment à partir duquel vous souhaitez rediriger les demandes (par exemple, `www.example.com`).
3. Choisissez Propriétés.
4. Sous Static website hosting (Hébergement de site web statique), choisissez Edit (Modifier).
5. Choisissez Redirect requests for an object (Rediriger les demandes pour un objet).
6. Dans la zone Host name (Nom d'hôte), entrez le point de terminaison du site web pour votre compartiment ou votre domaine personnalisé.

   Par exemple, si vous redirigez les demandes vers une adresse de domaine racine, entrez **`example.com`**.
7. Pour Protocol (Protocole), choisissez le protocole pour les demandes redirigées (none (aucun),http ou https).

   Si vous ne spécifiez pas de protocole, l'option par défaut est none (aucun).
8. Sélectionnez Enregistrer les modifications.

Configurer des règles de redirection pour utiliser des redirections conditionnelles avancées

Avec les règles de redirection avancées, vous pouvez acheminer des demandes de façon conditionnelle, en fonction de noms de clés d'objets spécifiques, de préfixes dans la demande ou de codes réponse. A titre d'exemple, supposez que vous supprimiez ou renommiez un objet dans votre compartiment. Vous pouvez ajouter une règle de routage qui redirige la demande vers un autre objet. Si vous souhaitez qu'un dossier ne soit plus accessible, vous pouvez ajouter une règle de routage pour rediriger la demande vers une autre page Web. Vous pouvez également ajouter une règle de routage pour gérer des conditions d'erreur en acheminant les demandes qui renvoient l'erreur vers un autre domaine, où celle-ci sera traitée.

Lorsque vous activez l'hébergement de site web statique pour votre compartiment, vous pouvez éventuellement spécifier des règles de redirection avancées. Amazon S3 impose une limitation de 50 règles de routage par configuration de site web. Si vous avez besoin de plus de 50 règles de routage, vous pouvez utiliser la redirection d'objet. Pour de plus amples informations, veuillez consulter Utilisation de la console S3.

Pour plus d'informations sur la configuration des règles de routage à l'aide de l'API REST, consultez PutBucketWebsitele manuel Amazon Simple Storage Service API Reference.

> **Important**
>
> Pour créer des règles de redirection dans la nouvelle console Amazon S3, vous devez utiliser JSON. Pour des exemples JSON, consultez Exemples de règles de redirection.

Pour configurer des règles de redirection pour un site web statique

Pour ajouter des règles de redirection pour un compartiment qui a déjà l'hébergement de site Web statique activé, procédez comme suit.

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom d'un compartiment que vous avez configuré en tant que site Web statique.
4. Choisissez Propriétés.

5. Sous Static website hosting (Hébergement de site Web statique), choisissez Edit (Modifier).
6. Dans la zone Redirection rules (Règles de redirection), entrez vos règles de redirection dans JSON.

   Dans la console S3, vous décrivez les règles en utilisant JSON. Pour des exemples JSON, consultez Exemples de règles de redirection. Amazon S3 impose une limitation de 50 règles de routage par configuration de site web.
7. Sélectionnez Enregistrer les modifications.

Éléments de règle de routage

Voici la syntaxe générale permettant de définir les règles de routage dans une configuration de site Web en JSON et XML Pour configurer les règles de redirection dans la nouvelle console S3, vous devez utiliser JSON. Pour des exemples JSON, consultez Exemples de règles de redirection.

JSON

```
[
    {
      "Condition": {
        "HttpErrorCodeReturnedEquals": "string",
        "KeyPrefixEquals": "string"
      },
      "Redirect": {
        "HostName": "string",
        "HttpRedirectCode": "string",
        "Protocol": "http"|"https",
        "ReplaceKeyPrefixWith": "string",
        "ReplaceKeyWith": "string"
      }
    }
  ]

Note: Redirect must each have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

XML

```
<RoutingRules> =
    <RoutingRules>
```

```
          <RoutingRule>...</RoutingRule>
          [<RoutingRule>...</RoutingRule>
          ...]
     </RoutingRules>

<RoutingRule> =
   <RoutingRule>
      [ <Condition>...</Condition> ]
      <Redirect>...</Redirect>
   </RoutingRule>

<Condition> =
   <Condition>
      [ <KeyPrefixEquals>...</KeyPrefixEquals> ]
      [ <HttpErrorCodeReturnedEquals>...</HttpErrorCodeReturnedEquals> ]
   </Condition>
    Note: <Condition> must have at least one child element.

<Redirect> =
   <Redirect>
      [ <HostName>...</HostName> ]
      [ <Protocol>...</Protocol> ]
      [ <ReplaceKeyPrefixWith>...</ReplaceKeyPrefixWith>  ]
      [ <ReplaceKeyWith>...</ReplaceKeyWith> ]
      [ <HttpRedirectCode>...</HttpRedirectCode> ]
   </Redirect>

Note: <Redirect> must have at least one child element. You can have either
 ReplaceKeyPrefix with or ReplaceKeyWith but not both.
```

Le tableau suivant décrit les éléments de la règle de routage.

Nom	Description
`RoutingRules`	Conteneur de l'ensemble des éléments `RoutingRule` .
`RoutingRule`	Une règle qui identifie une condition et la redirection qui est appliquée quand la condition est respectée. Condition :

Nom	Description
	• un conteneur `RoutingRules` doit comprendre au moins une règle de routage.
`Condition`	Conteneur de la description de la condition qui doit être respectée pour que la redirection spécifiée soit appliquée. Si la règle de routage ne comprend pas de condition, la règle s'applique à toutes les demandes.
`KeyPrefixEquals`	Le préfixe de nom de la clé d'objet à partir duquel les demandes sont redirigées. `KeyPrefixEquals` est requis si `HttpErrorCodeReturnedEquals` n'est pas spécifié. Si les deux paramètres `KeyPrefixEquals` et `HttpErrorCodeReturnedEquals` sont spécifiés, les deux doivent être vrais pour que la condition soit respectée.
`HttpErrorCodeReturnedEquals`	Le code d'erreur HTTP doit correspondre pour que la redirection s'applique. En cas d'erreur, et si le code d'erreur correspond à cette valeur, la redirection spécifiée est appliquée. `HttpErrorCodeReturnedEquals` est requis si `KeyPrefixEquals` n'est pas spécifié. Si les deux paramètres `KeyPrefixEquals` et `HttpErrorCodeReturnedEquals` sont spécifiés, les deux doivent être vrais pour que la condition soit respectée.

Nom	Description
`Redirect`	Elément du conteneur qui fournit des instructions pour rediriger la demande. Vous pouvez rediriger les demandes vers un autre hôte ou une autre page ; vous pouvez également indiquer un autre protocole d'utilisation. Une règle `RoutingRule` doit avoir un élément `Redirect`. Un élément `Redirect` doit contenir au moins l'un des éléments enfants suivants : `Protocol`, `HostName`, `ReplaceKeyPrefixWith` , `ReplaceKeyWith` ou `HttpRedirectCode` .
`Protocol`	Le protocole, `http` or `https`, à utiliser dans l'en-tête `Location` renvoyé dans la réponse. Si l'un des enfants est fourni, `Protocol` n'est pas requis.
`HostName`	Le nom d'hôte à utiliser dans l'en-tête `Location` qui est renvoyé dans la réponse. Si l'un des enfants est fourni, `HostName` n'est pas requis.
`ReplaceKeyPrefixWith`	Le préfixe de nom de la clé d'objet qui remplace la valeur de `KeyPrefixEquals` dans la demande de redirection. Si l'un des enfants est fourni, `ReplaceKeyPrefixWith` n'est pas requis. Il peut être fourni uniquement si `ReplaceKeyWith` n'est pas fourni.
`ReplaceKeyWith`	La clé de l'objet à utiliser dans l'en-tête `Location` qui est renvoyé dans la réponse. Si l'un des enfants est fourni, `ReplaceKeyWith` n'est pas requis. Il peut être fourni uniquement si `ReplaceKeyPrefixWith` n'est pas fourni.

Nom	Description
`HttpRedirectCode`	Le code de redirection HTTP à utiliser dans l'en-tête `Location` qui est renvoyé dans la réponse. Si l'un des enfants est fourni, `HttpRedirectCode` n'est pas requis.

Exemples de règles de redirection

Les exemples suivants décrivent les tâches de redirection courantes :

> **Important**
>
> Pour créer des règles de redirection dans la nouvelle console Amazon S3, vous devez utiliser JSON.

Example 1 : Redirection après renommage du préfixe de clé

Supposez que votre compartiment contienne les objets suivants :

- index.html
- docs/article1.html
- docs/article2.html

Vous décidez de remplacer le nom de dossier `docs/` par `documents/`. Après avoir fait ce changement, vous devez rediriger les demandes pour le préfixe `docs/` vers `documents/`. A titre d'exemple, la demande pour `docs/article1.html` sera redirigée vers `documents/article1.html`.

Dans ce cas, vous ajoutez la règle de routage suivante à la configuration du site web.

JSON

```
[
    {
```

```
        "Condition": {
            "KeyPrefixEquals": "docs/"
        },
        "Redirect": {
            "ReplaceKeyPrefixWith": "documents/"
        }
    }
]
```

XML

```
  <RoutingRules>
    <RoutingRule>
    <Condition>
      <KeyPrefixEquals>docs/</KeyPrefixEquals>
    </Condition>
    <Redirect>
      <ReplaceKeyPrefixWith>documents/</ReplaceKeyPrefixWith>
    </Redirect>
    </RoutingRule>
  </RoutingRules>
```

Example 2 : Redirection des demandes pour un répertoire supprimé vers une page

Supposez que vous supprimiez le dossier `images/`(c'est-à-dire tous les objets ayant le préfixe de clé `images/`). Vous pouvez ajouter une règle de routage qui redirige les demandes concernant tout objet ayant le préfixe de clé `images/` vers une page appelée `folderdeleted.html`.

JSON

```
[
    {
        "Condition": {
            "KeyPrefixEquals": "images/"
        },
        "Redirect": {
            "ReplaceKeyWith": "folderdeleted.html"
        }
    }
]
```

XML

```
<RoutingRules>
  <RoutingRule>
  <Condition>
     <KeyPrefixEquals>images/</KeyPrefixEquals>
  </Condition>
  <Redirect>
    <ReplaceKeyWith>folderdeleted.html</ReplaceKeyWith>
  </Redirect>
  </RoutingRule>
</RoutingRules>
```

Example 3 : Redirection d'une erreur HTTP

Supposons que lorsqu'un objet demandé n'est pas trouvé, vous souhaitiez rediriger les demandes vers une instance Amazon Elastic Compute Cloud (Amazon EC2). Ajoutez une règle de redirection afin que lorsqu'un code d'état HTTP 404 (Not Found) est renvoyé, le visiteur du site soit redirigé vers une EC2 instance Amazon qui gère la demande.

L'exemple suivant insère également le préfixe de la clé d'objet `report-404/` dans la redirection. Par exemple, si vous demandez une page `ExamplePage.html` et que cela entraîne une erreur HTTP 404, la demande est redirigée vers une `report-404/ExamplePage.html` page de l' EC2instance Amazon spécifiée. S'il n'y a pas de règle de routage et qu'une erreur HTTP 404 se produit, le document d'erreur spécifié dans la configuration est renvoyé.

JSON

```
[
    {
        "Condition": {
            "HttpErrorCodeReturnedEquals": "404"
        },
        "Redirect": {
            "HostName": "ec2-11-22-333-44.compute-1.amazonaws.com",
            "ReplaceKeyPrefixWith": "report-404/"
        }
    }
]
```

XML

```
<RoutingRules>
  <RoutingRule>
  <Condition>
    <HttpErrorCodeReturnedEquals>404</HttpErrorCodeReturnedEquals >
  </Condition>
  <Redirect>
    <HostName>ec2-11-22-333-44.compute-1.amazonaws.com</HostName>
    <ReplaceKeyPrefixWith>report-404/</ReplaceKeyPrefixWith>
  </Redirect>
  </RoutingRule>
</RoutingRules>
```

Rediriger les demandes pour un objet

Vous pouvez rediriger les demandes d'un objet vers un autre objet ou une autre URL en définissant l'emplacement de redirection du site Web dans les métadonnées de l'objet. Vous configurez la redirection en ajoutant la propriété `x-amz-website-redirect-location` aux métadonnées d'objet. Sur la console Amazon S3, vous définissez l'élément Website Redirect Location (Emplacement de redirection de site web) dans les métadonnées de l'objet. Si vous utilisez l'API Amazon S3, vous définissez `x-amz-website-redirect-location`. Le site web interprète alors l'objet comme une redirection 301.

Pour rediriger une demande vers un autre objet, vous définissez l'emplacement de redirection vers la clé de l'objet cible. Pour rediriger une demande vers une URL externe, vous définissez l'emplacement de redirection vers l'URL choisie. Pour plus d'informations sur les métadonnées d'objet, consultez Métadonnées d'objet définies par le système.

Quand vous définissez une redirection de page, vous pouvez garder ou supprimer le contenu de l'objet source. Par exemple, si vous avez un objet `page1.html` dans votre compartiment, vous pouvez rediriger toutes les demandes de cette page vers un autre objet, `page2.html`. Vous avez deux options :

- Conservez le contenu de l'objet `page1.html` et redirigez les demandes de pages.
- Supprimez le contenu de `page1.html` et chargez un objet zéro octet nommé `page1.html` pour remplacer l'objet existant et rediriger les demandes de pages.

Utilisation de la console S3

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la liste Compartiments, choisissez le nom d'un compartiment que vous avez configuré en tant que site web statique (par exemple, `example.com`).
3. Sous Objects (Objets), sélectionnez votre objet.
4. Choisissez Actions, puis Edit metadata (Modifier les métadonnées).
5. Choisissez Métadonnées.
6. Sélectionnez Ajouter des métadonnées.
7. Sous Type, choisissez System Defined (Défini par le système).
8. Dans Key, choisissez x-amz-website-redirect-location.
9. Dans Valeur, entrez le nom de clé de l'objet vers lequel vous souhaitez rediriger, par exemple `/page2.html`.

   Pour un autre objet dans le même compartiment, le préfixe `/` dans la valeur est requis. Vous pouvez également définir la valeur sur une URL externe, par exemple, `http://www.example.com`.
10. Choisissez Edit metadata (Modifier les métadonnées).

Utilisation de l'API REST

Les actions d'API Amazon S3 suivantes prennent en charge l'en-tête `x-amz-website-redirect-location` dans la demande. Amazon S3 stocke la valeur de l'en-tête dans les métadonnées de l'objet sous la forme `x-amz-website-redirect-location`.

- PUT Object
- Lancement du chargement partitionné
- POST Object
- PUT Object - Copy

Un compartiment configuré pour l'hébergement d'un site Web a un point de terminaison de site Web et un point de terminaison REST. Une demande pour une page qui est configurée comme une redirection 301 peut engendrer les résultats possibles suivants, selon le point de terminaison de la demande :

- Point de terminaison de site web propre à une Région – Amazon S3 redirige la demande de page en fonction de la valeur de la propriété `x-amz-website-redirect-location`.
- Point de terminaison REST – Amazon S3 ne redirige pas la demande de page. Il renvoie l'objet demandé.

Pour plus d'informations sur les points de terminaison, consultez Différences clés entre un point de terminaison de site web et un point de terminaison de l'API REST.

Lors de la définition d'une redirection de page, vous pouvez garder ou supprimer le contenu de l'objet source. A titre d'exemple, supposez que vous ayez un objet `page1.html` dans votre compartiment.

- Pour conserver le contenu de `page1.html` et rediriger uniquement les demandes de page, vous pouvez envoyer une demande PUT Object - Copy pour créer un objet `page1.html` qui utilise l'objet `page1.html` existant comme source. Dans votre demande, vous définissez l'en-tête `x-amz-website-redirect-location`. Lorsque la demande est terminée, la page d'origine et son contenu restent inchangés, cependant Amazon S3 redirige toute demande de la page vers l'emplacement de redirection que vous avez indiqué.
- Pour supprimer le contenu de l'objet `page1.html` et rediriger les demandes pour la page, vous pouvez envoyer une demande PUT Object pour charger un objet de 0 octet ayant la même clé d'objet : `page1.html`. Dans une demande PUT, vous définissez `x-amz-website-redirect-location` pour `page1.html`dans le nouvel objet. Une fois que la demande est terminée, `page1.html` n'a aucun contenu, et les demandes sont redirigées vers l'emplacement qui est spécifié par `x-amz-website-redirect-location`.

Lorsque vous récupérez l'objet à l'aide de l'action GET Object avec les autres métadonnées d'objet, Amazon S3 renvoie l'en-tête `x-amz-website-redirect-location` dans la réponse.

Utilisation du partage des ressources entre origines multiples (CORS)

Le partage des ressources cross-origin (CORS) définit un moyen pour les applications Web clientes chargées dans un domaine particulier d'interagir avec les ressources d'un autre domaine. Le CORS vous permet de créer de riches applications web côté client avec Amazon S3 et d'autoriser de manière sélective un accès cross-origin à vos ressources Amazon S3.

Cette section fournit une présentation du CORS. Les sous-rubriques décrivent comment activer CORS à l'aide de la console Amazon S3 ou par programmation à l'aide de l'API REST Amazon S3 et du. AWS SDKs

Partage des ressources de plusieurs origines : scénarios de cas d'utilisation

Les exemples de scénarios suivants utilisent le partage CORS.

Scénario 1

Supposons que vous hébergiez un site Internet dans un compartiment Amazon S3 appelé `website`, comme décrit dans Hébergement d'un site Web statique à l'aide d'Amazon S3. Les utilisateurs chargent le point de terminaison du site web :

```
http://website.s3-website.us-east-1.amazonaws.com
```

Vous souhaitez maintenant utiliser les pages Web stockées dans ce compartiment pour pouvoir effectuer des requêtes GET et PUT authentifiées JavaScript sur le même compartiment en utilisant le point de terminaison de l'API Amazon S3 pour le compartiment,. `website.s3.us-east-1.amazonaws.com` Un navigateur bloque normalement l'autorisation JavaScript de ces demandes, mais avec CORS, vous pouvez configurer votre compartiment pour activer explicitement les demandes provenant de différentes origines. `website.s3-website.us-east-1.amazonaws.com`

Scénario 2

Supposons que vous souhaitez héberger une police web à partir de votre compartiment S3. Une fois encore, les navigateurs requièrent un contrôle CORS (aussi appelé contrôle en amont) pour le chargement des polices web. Vous configurez le compartiment qui héberge la police web pour permettre à toute origine d'effectuer ces demandes.

Comment Amazon S3 évalue la configuration CORS sur un compartiment ?

Lorsque Amazon S3 reçoit une demande en amont d'un navigateur, il évalue la configuration CORS du compartiment et utilise la première règle `CORSRule` qui correspond à la demande entrante du navigateur pour permettre une demande cross-origin. Pour qu'une règle corresponde, les conditions suivantes doivent être remplies :

- L'en-tête `Origin` d'une demande CORS adressée à votre compartiment doit correspondre aux origines de l'élément `AllowedOrigins` de votre configuration CORS.

- Les méthodes HTTP spécifiées dans `Access-Control-Request-Method` dans une demande CORS adressée à votre compartiment doivent correspondre à la ou aux méthodes répertoriées dans l'élément `AllowedMethods` de votre configuration CORS.
- Les en-têtes répertoriés dans l'en-tête `Access-Control-Request-Headers` d'une demande de contrôle en amont doivent correspondre aux en-têtes de l'élément `AllowedHeaders` de votre configuration CORS.

> **Note**
>
> Les politiques ACLs et continuent de s'appliquer lorsque vous activez CORS sur votre compartiment.

Comment le point d'accès Object Lambda prend en charge le CORS

Quand S3 Object Lambda reçoit une demande d'un navigateur ou que la demande inclut un en-tête `Origin`, S3 Object Lambda ajoute toujours un champ d'en-tête `"AllowedOrigins":"*"`.

Pour plus d'informations sur l'utilisation du CORS, consultez les rubriques suivantes.

Rubriques

- Éléments d'une configuration CORS
- Configuration du partage des ressources entre origines multiples (CORS)
- Test du CORS
- Dépannage du CORS

Éléments d'une configuration CORS

Pour configurer le compartiment afin qu'il autorise les demandes cross-origin, vous créez une configuration CORS. La configuration CORS est un document contenant les éléments identifiant les origines auxquelles vous autorisez l'accès à votre compartiment, les opérations (méthodes HTTP) prises en charge pour chaque origine, et d'autres informations propres aux opérations. Vous pouvez ajouter jusqu'à 100 règles à la configuration. Vous pouvez ajouter la configuration CORS en tant que sous-ressource `cors` au compartiment.

Si vous configurez le CORS dans la console S3, vous devez utiliser JSON pour créer une configuration CORS. La nouvelle console S3 ne prend en charge que les configurations JSON CORS.

Pour plus d'informations sur la configuration CORS et les éléments qu'elle contient, consultez les rubriques ci-dessous. Pour savoir comment ajouter une configuration CORS, consultez Configuration du partage des ressources entre origines multiples (CORS).

> **Important**
>
> Dans la console S3, la configuration CORS doit être de type JSON.

Rubriques

- Élément AllowedMethods
- Élément AllowedOrigins
- Élément AllowedHeaders
- Élément ExposeHeaders
- Élément MaxAgeSeconds
- Exemples de configurations CORS

Élément **`AllowedMethods`**

Dans la configuration CORS, vous pouvez spécifier les valeurs suivantes pour l'élément `AllowedMethods`.

- GET
- PUT
- POST
- DELETE
- HEAD

Élément **`AllowedOrigins`**

Dans l'élément `AllowedOrigins`, vous spécifiez les origines à partir desquelles vous souhaitez autoriser des demandes cross-domaine, par exemple, `http://www.example.com`. La chaîne

de caractères d'origine peut contenir au maximum un caractère générique `*`, comme `http://*.example.com`. Si vous le souhaitez, vous pouvez spécifier `*` comme l'origine pour permettre à toutes les origines d'envoyer des demandes cross-origin. Vous pouvez également spécifier `https` pour permettre uniquement les origines sécurisées.

Élément **`AllowedHeaders`**

L'élément `AllowedHeaders` spécifie les en-têtes autorisés dans une demande en amont via l'en-tête `Access-Control-Request-Headers`. Chaque nom d'en-tête dans l'en-tête `Access-Control-Request-Headers` doit correspondre à une entrée dans l'élément. Amazon S3 envoie uniquement dans une réponse les en-têtes autorisés qui ont été demandés. Pour obtenir un exemple de liste d'en-têtes pouvant être utilisés dans les demandes adressées à Amazon S3, veuillez accéder à En-têtes de demande courants dans la Référence d'API Amazon Simple Storage Service.

Chaque AllowedHeaders chaîne de votre configuration peut contenir au plus un caractère générique *. Par exemple, `<AllowedHeader>x-amz-*</AllowedHeader>` permet tous les en-têtes propres à Amazon.

Élément **`ExposeHeaders`**

Chaque `ExposeHeader` élément identifie un en-tête dans la réponse auquel vous souhaitez que les clients puissent accéder depuis leurs applications (par exemple, depuis un JavaScript `XMLHttpRequest` objet). Pour obtenir la liste des en-têtes de réponse Amazon S3 courants, veuillez accéder à En-têtes de réponse courants dans la Référence d'API Amazon Simple Storage.

Élément **`MaxAgeSeconds`**

L'élément `MaxAgeSeconds` spécifie le nombre d'heures en secondes pendant lesquelles le navigateur peut mettre en cache une réponse pour une demande en amont comme identifié par la ressource, la méthode HTTP et l'origine.

Exemples de configurations CORS

Au lieu d'accéder à un site web en utilisant un point de terminaison de site web Amazon S3, vous pouvez utiliser votre propre domaine, comme `example1.com`, pour proposer votre contenu. Pour plus d'informations sur l'utilisation de votre propre domaine, consultez Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53.

L'exemple de configuration CORS suivant possède trois règles, qui sont spécifiées en tant qu'éléments `CORSRule` :

- La première règle autorise des demandes cross-origin PUT, POST et DELETE de l'origine `http://www.example1.com`. La règle autorise également tous les en-têtes dans une demande OPTIONS en amont via l'en-tête `Access-Control-Request-Headers`. En réponse à toute demande OPTIONS en amont, Amazon S3 renvoie les en-têtes demandés.
- La deuxième règle autorise les mêmes demandes cross-origin que la première, mais elle s'applique à une autre origine, `http://www.example2.com`.
- La troisième règle permet des demandes GET cross-origin de toutes les origines. Le caractère générique * fait référence à toutes les origines.

JSON

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders": []
    },
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example2.com"
        ],
        "ExposeHeaders": []
    },
    {
```

```
        "AllowedHeaders": [],
        "AllowedMethods": [
            "GET"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "ExposeHeaders": []
    }
]
```

XML

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example1.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>http://www.example2.com</AllowedOrigin>

   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>

   <AllowedHeader>*</AllowedHeader>
 </CORSRule>
 <CORSRule>
   <AllowedOrigin>*</AllowedOrigin>
   <AllowedMethod>GET</AllowedMethod>
 </CORSRule>
</CORSConfiguration>
```

La configuration CORS permet également d'ajouter des paramètres facultatifs, comme illustré dans la configuration CORS suivante. Dans cet exemple, la configuration CORS permet les demandes PUT, POST et DELETE cross-origin depuis l'origine `http://www.example.com`.

JSON

```
[
    {
        "AllowedHeaders": [
            "*"
        ],
        "AllowedMethods": [
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example.com"
        ],
        "ExposeHeaders": [
            "x-amz-server-side-encryption",
            "x-amz-request-id",
            "x-amz-id-2"
        ],
        "MaxAgeSeconds": 3000
    }
]
```

XML

```
<CORSConfiguration>
 <CORSRule>
   <AllowedOrigin>http://www.example.com</AllowedOrigin>
   <AllowedMethod>PUT</AllowedMethod>
   <AllowedMethod>POST</AllowedMethod>
   <AllowedMethod>DELETE</AllowedMethod>
   <AllowedHeader>*</AllowedHeader>
  <MaxAgeSeconds>3000</MaxAgeSeconds>
  <ExposeHeader>x-amz-server-side-encryption</
ExposeHeader>
  <ExposeHeader>x-amz-request-id</
ExposeHeader>
  <ExposeHeader>x-amz-id-2</ExposeHeader>
 </CORSRule>
</CORSConfiguration>
```

L'élément `CORSRule` dans la configuration précédente inclut les éléments facultatifs suivants :

- `MaxAgeSeconds` : spécifie le nombre d'heures en secondes (dans cet exemple, 3 000) pendant lesquelles le navigateur met en cache une réponse Amazon S3 à une demande OPTIONS en amont pour la ressource spécifiée. Le fait de mettre en cache la réponse évite au navigateur de devoir envoyer les demandes en amont à Amazon S3 si la demande originale est répétée.
- `ExposeHeaders`—Identifie les en-têtes de réponse (dans cet exemple`x-amz-server-side-encryption`,`x-amz-request-id`, et`x-amz-id-2`) auxquels les clients peuvent accéder depuis leurs applications (par exemple, depuis un JavaScript `XMLHttpRequest` objet).

Configuration du partage des ressources entre origines multiples (CORS)

Le partage des ressources cross-origin (CORS) définit un moyen pour les applications Web clientes chargées dans un domaine particulier d'interagir avec les ressources d'un autre domaine. Le CORS vous permet de créer de riches applications web côté client avec Amazon S3 et d'autoriser de manière sélective un accès cross-origin à vos ressources Amazon S3.

Cette section explique comment activer CORS à l'aide de la console Amazon S3, de l'API REST Amazon S3 et du AWS SDKs. Pour configurer le compartiment afin d'autoriser les demandes entre origines multiples, vous devez ajouter une configuration CORS au compartiment. Une configuration CORS est un document qui définit les règles identifiant les origines auxquelles vous autorisez l'accès au compartiment, les opérations (méthodes HTTP) prises en charge pour chaque origine, et d'autres informations propres aux opérations. Dans la console S3, la configuration CORS doit être un document JSON.

Pour obtenir un exemple de configurations CORS en JSON et XML, consultez Éléments d'une configuration CORS.

Utilisation de la console S3

Cette section explique comment utiliser la console Amazon S3 pour ajouter une configuration CORS (partage des ressources cross-origin) à un compartiment S3.

Lorsque vous activez CORS sur le bucket, les listes de contrôle d'accès (ACLs) et les autres politiques d'autorisation d'accès continuent de s'appliquer.

> **Important**
>
> Dans la console S3, la configuration CORS doit être de type JSON. Pour obtenir des exemples de configurations CORS en JSON et XML, consultez Éléments d'une configuration CORS.

Pour ajouter une configuration CORS à un compartiment S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez créer une politique de compartiment.
4. Choisissez Permissions.
5. Dans la section Partage des ressources cross-origin (CORS), choisissez Modifier.
6. Dans la zone de texte Editeur de configuration CORS, tapez ou copiez et collez une nouvelle configuration CORS, ou modifiez une configuration existante.

   La configuration CORS est un fichier JSON. Le texte que vous saisissez dans l'éditeur doit être dans un format JSON valide. Pour plus d'informations, consultez Éléments d'une configuration CORS.
7. Sélectionnez Save Changes (Enregistrer les modifications).

   > **Note**
   >
   > Amazon S3 affiche l'Amazon Resource Name (ARN) du compartiment en regard du titre Editeur de configuration CORS. Pour plus d'informations sur ARNs, consultez Amazon Resource Names (ARNs) et les espaces de noms de AWS service dans le Référence générale d'Amazon Web Services.

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDK pour gérer le partage de ressources entre origines (CORS) pour un bucket. Pour plus d'informations sur le CORS, consultez Utilisation du partage des ressources entre origines multiples (CORS).

Les exemples suivants :

- Crée une configuration CORS et définit la configuration sur un compartiment
- Récupère une configuration et la modifie en ajoutant une règle
- Ajoute la configuration modifiée au compartiment
- Supprime la configuration

Java

Example

Example

Pour obtenir des instructions sur la création et le test d'un échantillon fonctionnel, consultez Getting Started dans le guide du AWS SDK pour Java développeur.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.auth.profile.ProfileCredentialsProvider;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.BucketCrossOriginConfiguration;
import com.amazonaws.services.s3.model.CORSRule;

import java.io.IOException;
import java.util.ArrayList;
import java.util.Arrays;
import java.util.List;

public class CORS {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String bucketName = "*** Bucket name ***";

        // Create two CORS rules.
        List<CORSRule.AllowedMethods> rule1AM = new
 ArrayList<CORSRule.AllowedMethods>();
        rule1AM.add(CORSRule.AllowedMethods.PUT);
        rule1AM.add(CORSRule.AllowedMethods.POST);
```

```
        rule1AM.add(CORSRule.AllowedMethods.DELETE);
        CORSRule rule1 = new
CORSRule().withId("CORSRule1").withAllowedMethods(rule1AM)
                .withAllowedOrigins(Arrays.asList("http://*.example.com"));

        List<CORSRule.AllowedMethods> rule2AM = new
ArrayList<CORSRule.AllowedMethods>();
        rule2AM.add(CORSRule.AllowedMethods.GET);
        CORSRule rule2 = new
CORSRule().withId("CORSRule2").withAllowedMethods(rule2AM)
                .withAllowedOrigins(Arrays.asList("*")).withMaxAgeSeconds(3000)
                .withExposedHeaders(Arrays.asList("x-amz-server-side-encryption"));

        List<CORSRule> rules = new ArrayList<CORSRule>();
        rules.add(rule1);
        rules.add(rule2);

        // Add the rules to a new CORS configuration.
        BucketCrossOriginConfiguration configuration = new
BucketCrossOriginConfiguration();
        configuration.setRules(rules);

        try {
            AmazonS3 s3Client = AmazonS3ClientBuilder.standard()
                    .withCredentials(new ProfileCredentialsProvider())
                    .withRegion(clientRegion)
                    .build();

            // Add the configuration to the bucket.
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

            // Retrieve and display the configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            printCORSConfiguration(configuration);

            // Add another new rule.
            List<CORSRule.AllowedMethods> rule3AM = new
ArrayList<CORSRule.AllowedMethods>();
            rule3AM.add(CORSRule.AllowedMethods.HEAD);
            CORSRule rule3 = new
CORSRule().withId("CORSRule3").withAllowedMethods(rule3AM)
                    .withAllowedOrigins(Arrays.asList("http://www.example.com"));

            rules = configuration.getRules();
```

```
            rules.add(rule3);
            configuration.setRules(rules);
            s3Client.setBucketCrossOriginConfiguration(bucketName, configuration);

            // Verify that the new rule was added by checking the number of rules in
the
            // configuration.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            System.out.println("Expected # of rules = 3, found " +
configuration.getRules().size());

            // Delete the configuration.
            s3Client.deleteBucketCrossOriginConfiguration(bucketName);
            System.out.println("Removed CORS configuration.");

            // Retrieve and display the configuration to verify that it was
            // successfully deleted.
            configuration = s3Client.getBucketCrossOriginConfiguration(bucketName);
            printCORSConfiguration(configuration);
        } catch (AmazonServiceException e) {
            // The call was transmitted successfully, but Amazon S3 couldn't process
            // it, so it returned an error response.
            e.printStackTrace();
        } catch (SdkClientException e) {
            // Amazon S3 couldn't be contacted for a response, or the client
            // couldn't parse the response from Amazon S3.
            e.printStackTrace();
        }
    }

    private static void printCORSConfiguration(BucketCrossOriginConfiguration
configuration) {
        if (configuration == null) {
            System.out.println("Configuration is null.");
        } else {
            System.out.println("Configuration has " +
configuration.getRules().size() + " rules\n");

            for (CORSRule rule : configuration.getRules()) {
                System.out.println("Rule ID: " + rule.getId());
                System.out.println("MaxAgeSeconds: " + rule.getMaxAgeSeconds());
                System.out.println("AllowedMethod: " + rule.getAllowedMethods());
                System.out.println("AllowedOrigins: " + rule.getAllowedOrigins());
                System.out.println("AllowedHeaders: " + rule.getAllowedHeaders());
```

```
                System.out.println("ExposeHeader: " + rule.getExposedHeaders());
                System.out.println();
            }
        }
    }
}
```

.NET

Example

Pour plus d'informations sur la configuration et l'exécution des exemples de code, consultez Getting Started with the AWS SDK for .NET dans AWS le Guide du développeur du SDK pour .NET.

```
using Amazon;
using Amazon.S3;
using Amazon.S3.Model;
using System;
using System.Collections.Generic;
using System.Threading.Tasks;

namespace Amazon.DocSamples.S3
{
    class CORSTest
    {
        private const string bucketName = "*** bucket name ***";
        // Specify your bucket region (an example region is shown).
        private static readonly RegionEndpoint bucketRegion =
 RegionEndpoint.USWest2;
        private static IAmazonS3 s3Client;

        public static void Main()
        {
            s3Client = new AmazonS3Client(bucketRegion);
            CORSConfigTestAsync().Wait();
        }
        private static async Task CORSConfigTestAsync()
        {
            try
            {
                // Create a new configuration request and add two rules
                CORSConfiguration configuration = new CORSConfiguration
```

```
                {
                    Rules = new System.Collections.Generic.List<CORSRule>
                        {
                          new CORSRule
                          {
                            Id = "CORSRule1",
                            AllowedMethods = new List<string> {"PUT", "POST",
 "DELETE"},
                            AllowedOrigins = new List<string> {"http://
*.example.com"}
                          },
                          new CORSRule
                          {
                            Id = "CORSRule2",
                            AllowedMethods = new List<string> {"GET"},
                            AllowedOrigins = new List<string> {"*"},
                            MaxAgeSeconds = 3000,
                            ExposeHeaders = new List<string> {"x-amz-server-side-
encryption"}
                          }
                        }
                };

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Retrieve an existing configuration.
                configuration = await RetrieveCORSConfigurationAsync();

                // Add a new rule.
                configuration.Rules.Add(new CORSRule
                {
                    Id = "CORSRule3",
                    AllowedMethods = new List<string> { "HEAD" },
                    AllowedOrigins = new List<string> { "http://www.example.com" }
                });

                // Add the configuration to the bucket.
                await PutCORSConfigurationAsync(configuration);

                // Verify that there are now three rules.
                configuration = await RetrieveCORSConfigurationAsync();
                Console.WriteLine();
```

```
                Console.WriteLine("Expected # of rulest=3; found:{0}",
configuration.Rules.Count);
                Console.WriteLine();
                Console.WriteLine("Pause before configuration delete. To continue,
click Enter...");
                Console.ReadKey();

                // Delete the configuration.
                await DeleteCORSConfigurationAsync();

                // Retrieve a nonexistent configuration.
                configuration = await RetrieveCORSConfigurationAsync();
            }
            catch (AmazonS3Exception e)
            {
                Console.WriteLine("Error encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
            catch (Exception e)
            {
                Console.WriteLine("Unknown encountered on server. Message:'{0}' when
writing an object", e.Message);
            }
        }

        static async Task PutCORSConfigurationAsync(CORSConfiguration configuration)
        {

            PutCORSConfigurationRequest request = new PutCORSConfigurationRequest
            {
                BucketName = bucketName,
                Configuration = configuration
            };

            var response = await s3Client.PutCORSConfigurationAsync(request);
        }

        static async Task<CORSConfiguration> RetrieveCORSConfigurationAsync()
        {
            GetCORSConfigurationRequest request = new GetCORSConfigurationRequest
            {
                BucketName = bucketName

            };
```

```
            var response = await s3Client.GetCORSConfigurationAsync(request);
            var configuration = response.Configuration;
            PrintCORSRules(configuration);
            return configuration;
        }

        static async Task DeleteCORSConfigurationAsync()
        {
            DeleteCORSConfigurationRequest request = new
DeleteCORSConfigurationRequest
            {
                BucketName = bucketName
            };
            await s3Client.DeleteCORSConfigurationAsync(request);
        }

        static void PrintCORSRules(CORSConfiguration configuration)
        {
            Console.WriteLine();

            if (configuration == null)
            {
                Console.WriteLine("\nConfiguration is null");
                return;
            }

            Console.WriteLine("Configuration has {0} rules:",
configuration.Rules.Count);
            foreach (CORSRule rule in configuration.Rules)
            {
                Console.WriteLine("Rule ID: {0}", rule.Id);
                Console.WriteLine("MaxAgeSeconds: {0}", rule.MaxAgeSeconds);
                Console.WriteLine("AllowedMethod: {0}", string.Join(", ",
rule.AllowedMethods.ToArray()));
                Console.WriteLine("AllowedOrigins: {0}", string.Join(", ",
rule.AllowedOrigins.ToArray()));
                Console.WriteLine("AllowedHeaders: {0}", string.Join(", ",
rule.AllowedHeaders.ToArray()));
                Console.WriteLine("ExposeHeader: {0}", string.Join(", ",
rule.ExposeHeaders.ToArray()));
            }
        }
    }
```

```
}
```

Utilisation de l'API REST

Pour définir une configuration CORS sur votre compartiment, vous pouvez utiliser AWS Management Console. Si l'application l'exige, vous pouvez également envoyer directement des demandes REST. Les sections suivantes de la Référence d'API Amazon Simple Storage Service décrivent les actions de l'API REST liées à la configuration CORS :

- PutBucketCors
- GetBucketCors
- DeleteBucketCors
- OPTIONS object

Test du CORS

Pour tester votre configuration CORS, une demande de contrôle en amont CORS peut être envoyée avec la méthode `OPTIONS` afin que le serveur puisse répondre s'il est acceptable d'envoyer la demande. Quand Amazon S3 reçoit une demande de contrôle en amont, S3 évalue la configuration CORS du compartiment et utilise la première règle `CORSRule` qui correspond à la demande entrante pour permettre une demande cross-origin. Pour qu'une règle corresponde, les conditions suivantes doivent être remplies :

- L'en-tête `Origin` d'une demande CORS adressée à votre compartiment doit correspondre aux origines de l'élément `AllowedOrigins` de votre configuration CORS.
- Les méthodes HTTP spécifiées dans `Access-Control-Request-Method` dans une demande CORS adressée à votre compartiment doivent correspondre à la ou aux méthodes répertoriées dans l'élément `AllowedMethods` de votre configuration CORS.
- Les en-têtes répertoriés dans l'en-tête `Access-Control-Request-Headers` d'une demande de contrôle en amont doivent correspondre aux en-têtes de l'élément `AllowedHeaders` de votre configuration CORS.

Voici un exemple de configuration CORS. Pour créer une configuration CORS, consultez Configuration de CORS. Pour plus d'exemples de configuration de CORS, consultez Éléments d'une configuration CORS.

Pour obtenir des conseils sur la configuration et le dépannage des règles CORS, consultez Comment configurer le CORS dans Amazon S3 et confirmer les règles CORS à l'aide de cURL ? dans le AWS re:Post Knowledge Center.

JSON

```
[
    {
        "AllowedHeaders": [
            "Authorization"
        ],
        "AllowedMethods": [
            "GET",
            "PUT",
            "POST",
            "DELETE"
        ],
        "AllowedOrigins": [
            "http://www.example1.com"
        ],
        "ExposeHeaders":  [
             "x-amz-meta-custom-header"
        ]

    }
]
```

Pour tester la configuration CORS, vous pouvez envoyer un contrôle `OPTIONS` en amont à l'aide de la commande CURL suivante. CURL est un outil de ligne de commande qui peut être utilisé pour interagir avec S3. Pour plus d'informations, consultez CURL.

```
curl -v -X OPTIONS \
 -H "Origin: http://www.example1.com" \
 -H "Access-Control-Request-Method: PUT" \
 -H "Access-Control-Request-Headers: Authorization" \
 -H "Access-Control-Expose-Headers: x-amz-meta-custom-header"\
    "http://bucket_name.s3.amazonaws.com/object_prefix_name"
```

Dans l'exemple ci-dessus, la commande `curl -v -x OPTIONS` est utilisée pour envoyer une demande de contrôle en amont à S3 afin de savoir si S3 autorise l'envoi d'une demande PUT sur un

objet à partir de l'adresse `http://www.example1.com` d'origines multiples. Les en-têtes `Access-Control-Request-Headers` et `Access-Control-Expose-Headers` sont facultatifs.

- En réponse à l'en-tête `Access-Control-Request-Method` de la demande `OPTIONS` de contrôle en amont, Amazon S3 renvoie la liste des méthodes autorisées si les méthodes demandées correspondent.
- En réponse à l'en-tête `Access-Control-Request-Headers` de la demande `OPTIONS` de contrôle en amont, Amazon S3 renvoie la liste des méthodes autorisées si les en-têtes demandés correspondent.
- En réponse à l'en-tête `Access-Control-Expose-Headers` de la demande `OPTIONS` de contrôle en amont, Amazon S3 renvoie la liste des en-têtes autorisés si les en-têtes demandés correspondent aux en-têtes autorisés accessibles par les scripts s'exécutant dans le navigateur.

> **Note**
>
> Lors de l'envoi d'une demande de contrôle en amont, si un ou des en-têtes de demande CORS ne sont pas autorisés, aucun des en-têtes CORS de réponse n'est renvoyé.

En réponse à cette demande `OPTIONS` de contrôle en amont, vous recevrez une réponse `200 OK`. Pour les codes d'erreur courants reçus lors du test du partage CORS et pour plus d'informations sur la résolution des problèmes liés au partage CORS, consultez Résolution des problèmes liés au CORS.

```
< HTTP/1.1 200 OK
< Date: Fri, 12 Jul 2024 00:23:51 GMT
< Access-Control-Allow-Origin: http://www.example1.com
< Access-Control-Allow-Methods: GET, PUT, POST, DELETE
< Access-Control-Allow-Headers: Authorization
< Access-Control-Expose-Headers: x-amz-meta-custom-header
< Access-Control-Allow-Credentials: true
< Vary: Origin, Access-Control-Request-Headers, Access-Control-Request-Method
< Server: AmazonS3
< Content-Length: 0
```

Dépannage du CORS

Les rubriques suivantes peuvent vous aider à résoudre certains problèmes CORS courants liés à S3.

Rubriques

- Erreur 403 Forbidden : CORS n'est pas activé pour ce compartiment
- Erreur 403 Forbidden : cette demande CORS n'est pas autorisée
- En-têtes introuvables dans la réponse CORS
- Considérations relatives à CORS sur les intégrations de proxy S3

Erreur 403 Forbidden : CORS n'est pas activé pour ce compartiment

L'erreur `403 Forbidden` suivante se produit lorsqu'une demande entre origines multiples est envoyée à Amazon S3 mais que CORS n'est pas configuré sur votre compartiment S3.

Erreur : HTTP/1.1 403 Forbidden CORS Response: CORS is not enabled for this bucket.

La configuration CORS est un document ou une politique contenant des règles qui identifient les origines auxquelles vous autorisez l'accès à votre compartiment, les opérations (méthodes HTTP) prises en charge pour chaque origine, et d'autres informations propres aux opérations. Découvrez comment configurer CORS sur S3 à l'aide de la console Amazon S3 et de l'API REST. AWS SDKs Pour plus d'informations sur CORS et des exemples de configuration CORS, consultez Éléments de CORS.

Erreur 403 Forbidden : cette demande CORS n'est pas autorisée

L'erreur `403 Forbidden` suivante est reçue lorsqu'une règle CORS de votre configuration CORS ne correspond pas aux données de votre demande.

Erreur : HTTP/1.1 403 Forbidden CORS Response: This CORS request is not allowed.

Par conséquent, cette erreur `403 Forbidden` peut se produire pour plusieurs raisons :

- L'origine n'est pas autorisée.
- Les méthodes ne sont pas autorisées.
- Les en-têtes demandés ne sont pas autorisés.

Pour chaque demande reçue par Amazon S3, vous devez disposer dans votre configuration CORS d'une règle CORS correspondant aux données de votre demande.

L'origine n'est pas autorisée

L'en-tête `Origin` d'une demande CORS adressée à votre compartiment doit correspondre aux origines de l'élément `AllowedOrigins` de votre configuration CORS. Un caractère générique (`"*"`) dans l'élément `AllowedOrigins` correspondrait à toutes les méthodes HTTP. Pour plus d'informations sur la façon de mettre à jour l'élément `AllowedOrigins`, consultez Configuration du partage des ressources entre origines multiples (CORS).

Par exemple, si seul le domaine `http://www.example1.com` est inclus dans l'élément `AllowedOrigins`, une demande CORS envoyée depuis le domaine `http://www.example2.com` recevra l'erreur `403 Forbidden`.

L'exemple suivant montre une partie d'une configuration CORS qui inclut le domaine `http://www.example1.com` dans l'élément `AllowedOrigins`.

```
"AllowedOrigins":[
   "http://www.example1.com"
]
```

Pour qu'une demande CORS envoyée depuis le domaine `http://www.example2.com` aboutisse, le domaine `http://www.example2.com` doit être inclus dans l'élément `AllowedOrigins` de la configuration CORS.

```
"AllowedOrigins":[
   "http://www.example1.com"
   "http://www.example2.com"
]
```

Les méthodes ne sont pas autorisées

Les méthodes HTTP spécifiées dans `Access-Control-Request-Method`, dans une demande CORS adressée à votre compartiment, doivent correspondre à la ou aux méthodes répertoriées dans l'élément `AllowedMethods` de votre configuration CORS. Un caractère générique (`"*"`) dans `AllowedMethods` correspondrait à toutes les méthodes HTTP. Pour plus d'informations sur la façon de mettre à jour l'élément `AllowedOrigins`, consultez Configuration du partage des ressources entre origines multiples (CORS).

Dans une configuration CORS, vous pouvez spécifier les méthodes suivantes dans l'élément `AllowedMethods` :

- GET
- PUT
- POST
- DELETE
- HEAD

L'exemple suivant montre une partie d'une configuration CORS qui inclut la méthode GET dans l'élément AllowedMethods. Seules les demandes incluant la méthode GET aboutiront.

```
"AllowedMethods":[
   "GET"
]
```

Si une méthode HTTP (par exemple, PUT) était utilisée dans une demande CORS ou incluse dans une demande CORS de contrôle en amont adressée à votre compartiment mais que la méthode n'était pas présente dans votre configuration CORS, la demande entraînerait une erreur 403 Forbidden. Pour autoriser cette demande CORS ou cette demande CORS de contrôle en amont, vous devez ajouter la méthode PUT à votre configuration CORS.

```
"AllowedMethods":[
   "GET"
   "PUT"
]
```

Les en-têtes demandés ne sont pas autorisés

Les en-têtes répertoriés dans l'en-tête Access-Control-Request-Headers d'une demande de contrôle en amont doivent correspondre aux en-têtes de l'élément AllowedHeaders de votre configuration CORS. Pour obtenir la liste des en-têtes courants qui peuvent être utilisés dans les demandes adressées à Amazon S3, consultez En-têtes de demandes courants. Pour plus d'informations sur la façon de mettre à jour l'élément AllowedHeaders, consultez Configuration du partage des ressources entre origines multiples (CORS).

L'exemple suivant montre une partie d'une configuration CORS qui inclut l'en-tête Authorization dans l'élément AllowedHeaders. Seules les demandes relatives à l'en-tête Authorization aboutiront.

```
"AllowedHeaders":  [
```

```
    "Authorization"
]
```

Si un en-tête (par exemple, `Content-MD5`) était inclus dans une demande CORS mais qu'il n'était pas présent dans votre configuration CORS, la demande entraînerait une erreur `403 Forbidden`. Pour autoriser cette demande CORS, vous devez ajouter l'en-tête `Content-MD5` à votre configuration CORS. Si vous souhaitez transmettre à la fois les en-têtes `Authorization` et `Content-MD5` dans une demande CORS à votre compartiment, vérifiez que les deux en-têtes sont inclus dans l'élément `AllowedHeaders` de votre configuration CORS.

```
"AllowedHeaders":  [
    "Authorization"
    "Content-MD5"
]
```

En-têtes introuvables dans la réponse CORS

L'élément `ExposeHeaders` de votre configuration CORS identifie les en-têtes de réponse que vous souhaiteriez rendre accessibles aux scripts et aux applications exécutés dans les navigateurs, en réponse à une demande CORS.

Si vos objets stockés dans votre compartiment S3 comportent des métadonnées définies par l'utilisateur (par exemple,`x-amz-meta-custom-header`) en plus des données de réponse, cet en-tête personnalisé peut contenir des métadonnées ou des informations supplémentaires auxquelles vous souhaitez accéder à partir de votre code côté client JavaScript . Toutefois, par défaut, les navigateurs bloquent l'accès aux en-têtes personnalisés pour des raisons de sécurité. Pour permettre à votre client JavaScript d'accéder aux en-têtes personnalisés, vous devez inclure l'en-tête dans votre configuration CORS.

Dans l'exemple ci-dessous, l'en-tête `x-amz-meta-custom-header1` est inclus dans l'élément `ExposeHeaders`. L'élément `x-amz-meta-custom-header2` n'est pas inclus dans l'élément `ExposeHeaders` et est absent de la configuration CORS. Dans la réponse, seules les valeurs incluses dans l'élément `ExposeHeaders` seraient renvoyées. Si la demande incluait l'en-tête `x-amz-meta-custom-header2` dans l'en-tête `Access-Control-Expose-Headers`, la réponse renverrait toujours un `200 OK`. Toutefois, seul l'en-tête autorisé (par exemple, `x-amz-meta-custom-header`) serait renvoyé et affiché dans la réponse.

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1"
```

```
]
```

Pour vous assurer que tous les en-têtes apparaîtront dans la réponse, ajoutez tous les en-têtes autorisés à l'élément `ExposeHeaders` dans votre configuration CORS, comme indiqué ci-dessous.

```
"ExposeHeaders":  [
    "x-amz-meta-custom-header1",
    "x-amz-meta-custom-header2"
]
```

Considérations relatives à CORS sur les intégrations de proxy S3

Si vous rencontrez des erreurs et que vous avez déjà vérifié la configuration CORS sur votre compartiment S3 et que la demande cross-origin est envoyée à des proxys tels que AWS CloudFront, essayez ce qui suit :

- Configurez les paramètres pour autoriser la méthode `OPTIONS` pour les requêtes HTTP.
- Configurez le proxy pour transférer les en-têtes suivants : `Origin`, `Access-Control-Request-Headers` et `Access-Control-Request-Method`.
- Configurez les paramètres du proxy pour inclure l'en-tête d'origine dans sa clé de cache. Ceci est important car les proxys de mise en cache qui n'incluent pas l'en-tête d'origine dans leur clé de cache peuvent fournir des réponses mises en cache qui n'incluent pas les en-têtes CORS appropriés pour différentes origines.

Certains proxys fournissent des fonctionnalités prédéfinies pour les demandes CORS. Par exemple, dans CloudFront, vous pouvez configurer une politique qui inclut les en-têtes

qui activent les demandes de partage de ressources entre origines multiples (CORS) lorsque l'origine est un compartiment Amazon S3.

Cette stratégie possède les paramètres suivants :

- En-têtes inclus dans les demandes d'origine :

  `Origin`

  `Access-Control-Request-Headers`

  `Access-Control-Request-Method`

- Cookies inclus dans les demandes d'origine : Aucun
- Chaînes de requête incluses dans les demandes d'origine : Aucune

Pour plus d'informations, consultez les sections Contrôler les demandes d'origine à l'aide d'une politique et Utiliser des politiques de demande d'origine gérées dans le Guide du CloudFront développeur.

Didacticiels relatifs aux sites Web statiques

Les didacticiels ou guides suivants présentent des procédures complètes de création et de configuration d'un compartiment Amazon S3 à usage général pour l'hébergement de sites Web statiques et l'hébergement de vidéos en streaming à la demande. L'objectif de ces didacticiels est de fournir des conseils généraux. Ces didacticiels sont destinés à un environnement de type atelier et utilisent des exemples de noms de compartiment, de noms d'utilisateur, etc. Ils ne sont pas conçus pour être utilisés directement dans votre environnement de production sans être préalablement vérifiés et adaptés soigneusement aux besoins uniques de votre organisation.

- Hébergement de vidéos en streaming à la demande avec Amazon S3 CloudFront, Amazon et Amazon Route 53 — Vous pouvez utiliser Amazon S3 avec Amazon pour héberger des vidéos destinées CloudFront à être visionnées à la demande de manière sécurisée et évolutive. Une fois que votre vidéo est empaquetée dans les bons formats, vous pouvez la stocker sur un serveur ou dans un compartiment S3 à usage général, puis la diffuser CloudFront selon les demandes des spectateurs. Dans ce didacticiel, vous allez apprendre à configurer votre bucket à usage général pour héberger du streaming vidéo à la demande en utilisant CloudFront pour la diffusion, Amazon Route 53 pour le système de noms de domaine (DNS) et la gestion personnalisée des domaines. CloudFront diffuse la vidéo depuis son cache et ne la récupère depuis votre compartiment à usage général que si elle n'est pas déjà mise en cache. Cette fonction de gestion de la mise en cache accélère la livraison de vos vidéos aux utilisateurs du monde entier avec une faible latence, un débit élevé et des vitesses de transfert élevées. Pour plus d'informations sur la gestion de CloudFront la mise en cache, consultez Optimisation de la mise en cache et de la disponibilité dans le manuel Amazon CloudFront Developer Guide.
- Configuration d'un site Web statique : vous pouvez configurer un compartiment à usage général afin qu'il fonctionne comme un site Web. Ce didacticiel explique les étapes de l'hébergement d'un site Web sur Amazon S3, notamment la création d'un compartiment, l'activation de l'hébergement des sites Web statiques dans la console S3, la création d'un document d'index et la création d'un

document d'erreur. Pour plus d'informations, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.

- Configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53 : vous pouvez créer et configurer un compartiment à usage général afin d'héberger un site Web statique et créer des redirections sur S3 pour un site Web avec un nom de domaine personnalisé, enregistré auprès d'Amazon Route 53. Vous utilisez Route 53 pour enregistrer les domaines et définir où vous souhaitez router le trafic Internet destiné à votre domaine. Ce didacticiel montre comment créer des enregistrements d'alias Route 53 pour router le trafic destiné à votre domaine et à votre sous-domaine vers votre compartiment à usage général, qui contient un fichier HTML. Pour plus d'informations, consultez Utilisation de votre domaine pour un site Web statique dans un compartiment Amazon S3 dans le Guide du développeur Amazon Route 53. Après avoir terminé ce didacticiel, vous pouvez éventuellement l'utiliser CloudFront pour améliorer les performances de votre site Web. Pour plus d'informations, consultez Accélérer votre site Web avec Amazon CloudFront.
- Déploiement d'un site Web statique vers AWS Amplify Hosting à partir d'un compartiment S3 à usage général — Nous vous recommandons d'utiliser AWS Amplify Hosting pour héberger le contenu de site Web statique stocké sur S3. Amplify Hosting est un service entièrement géré qui facilite le déploiement de vos sites Web sur un réseau de diffusion de contenu (CDN) disponible dans le monde entier alimenté par Amazon CloudFront, permettant un hébergement de sites Web statique sécurisé sans configuration approfondie. Avec AWS Amplify Hosting, vous pouvez sélectionner l'emplacement de vos objets dans votre compartiment à usage général, déployer votre contenu sur un CDN géré et générer une URL HTTPS publique pour que votre site Web soit accessible partout. Pour plus d'informations, consultez Déploiement d'un site Web statique depuis S3 à l'aide de la console Amplify dans le Guide de l'utilisateur AWS Amplify Hosting.

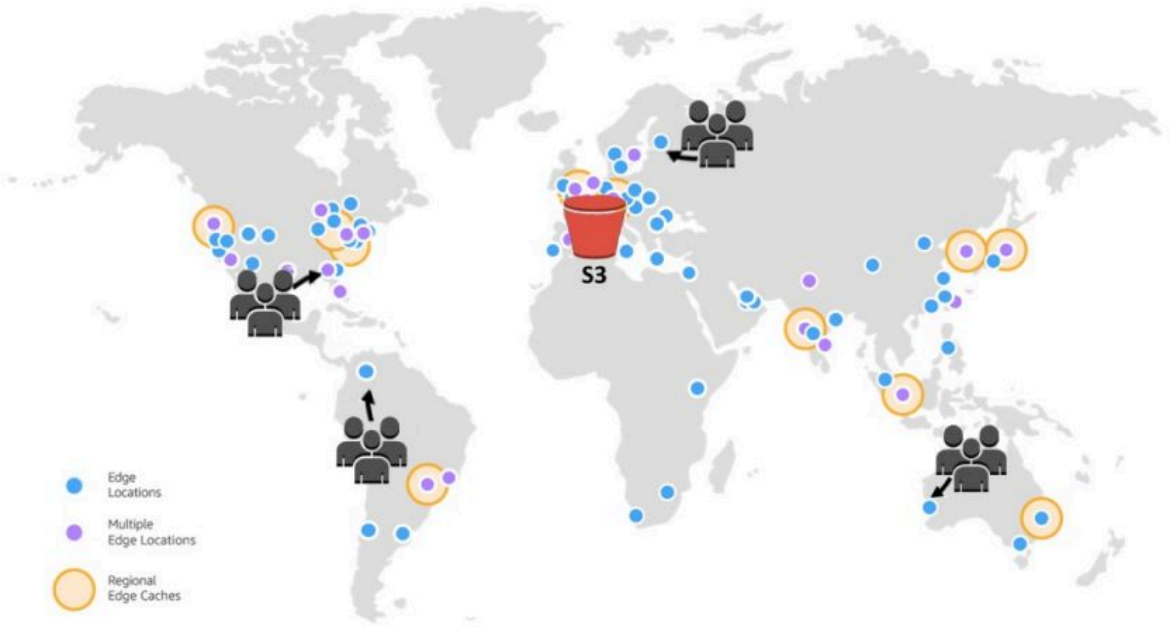
Tutoriel : Hébergement de vidéos en streaming à la demande avec Amazon S3 CloudFront, Amazon et Amazon Route 53

Vous pouvez utiliser Amazon S3 avec Amazon CloudFront pour héberger des vidéos à visionner à la demande de manière sécurisée et évolutive. Les vidéos en streaming à la demande (VOD) signifient votre contenu vidéo est stocké sur un serveur et que les utilisateurs peuvent les regarder à tout moment.

CloudFront est un service de réseau de diffusion de contenu (CDN) rapide, hautement sécurisé et programmable. CloudFront peut diffuser votre contenu en toute sécurité via HTTPS à partir de tous

les sites CloudFront périphériques du monde entier. Pour plus d'informations CloudFront, consultez Qu'est-ce qu'Amazon CloudFront ? dans le manuel Amazon CloudFront Developer Guide.

CloudFront la mise en cache réduit le nombre de demandes auxquelles votre serveur d'origine doit répondre directement. Lorsqu'un spectateur (utilisateur final) demande une vidéo que vous diffusez CloudFront, la demande est acheminée vers un emplacement périphérique proche de l'endroit où se trouve le spectateur. CloudFront diffuse la vidéo depuis son cache, en la récupérant du compartiment S3 uniquement si elle n'est pas déjà mise en cache. Cette fonction de gestion de la mise en cache accélère la livraison de vos vidéos aux utilisateurs du monde entier avec une faible latence, un débit élevé et des vitesses de transfert élevées. Pour plus d'informations sur la gestion de CloudFront la mise en cache, consultez Optimisation de la mise en cache et de la disponibilité dans le manuel Amazon CloudFront Developer Guide.



Objectif

Dans ce didacticiel, vous allez configurer un compartiment S3 pour héberger le streaming vidéo à la demande à l'aide CloudFront d'Amazon Route 53 pour le système de noms de domaine (DNS) et de la gestion personnalisée des domaines.

Rubriques

- Conditions préalables : enregistrez et configurez un domaine personnalisé avec Route 53

- Étape 1 : créer un compartiment S3
- Étape 2 : charger une vidéo dans le compartiment S3
- Étape 3 : créer une identité d'accès à l' CloudFront origine
- Étape 4 : Création d'une CloudFront distribution
- Étape 5 : Accédez à la vidéo via la CloudFront distribution
- Étape 6 : configurer votre CloudFront distribution pour utiliser votre nom de domaine personnalisé
- Étape 7 : Accédez à la vidéo S3 via la CloudFront distribution avec le nom de domaine personnalisé
- (Facultatif) Étape 8 : Afficher les données relatives aux demandes reçues par votre CloudFront distribution
- Étape 9 : nettoyer
- Étapes suivantes

Conditions préalables : enregistrez et configurez un domaine personnalisé avec Route 53

Avant de commencer ce didacticiel, vous devez enregistrer et configurer un domaine personnalisé (par exemple,**`example.com`**) avec Route 53 afin de pouvoir configurer votre CloudFront distribution pour utiliser un nom de domaine personnalisé ultérieurement.

Sans nom de domaine personnalisé, votre vidéo S3 est accessible CloudFront au public et hébergée via une URL similaire à la suivante :

```
https://CloudFront distribution domain name/Path to an S3 video
```

Par exemple, **`https://d111111abcdef8.cloudfront.net/sample.mp4`**.

Une fois que vous avez configuré votre CloudFront distribution pour utiliser un nom de domaine personnalisé configuré avec Route 53, votre vidéo S3 est accessible CloudFront au public et hébergée via une URL similaire à la suivante :

```
https://CloudFront distribution alternate domain name/Path to an S3 video
```

Par exemple, **`https://www.example.com/sample.mp4`**. Un nom de domaine personnalisé est plus simple et plus intuitif pour les utilisateurs.

Pour enregistrer un domaine personnalisé, consultez Enregistrement d'un nouveau domaine avec Route 53 dans le Guide du développeur Amazon Route 53.

Si vous enregistrez un nom de domaine avec Route 53, Route 53 créera pour vous la zone hébergée que vous utiliserez ultérieurement dans ce didacticiel. Cette zone hébergée est l'endroit où vous stockez des informations sur la manière d'acheminer le trafic de votre domaine, par exemple vers une EC2 instance Amazon ou une CloudFront distribution.

Des frais sont associés à l'enregistrement de domaine, à votre zone hébergée et aux requêtes DNS reçues par votre domaine. Pour plus d'informations, consultez Tarification Amazon Route 53.

> **Note**
>
> Lorsque vous enregistrez un domaine, cela coûte immédiatement de l'argent et c'est irréversible. Vous pouvez choisir de ne pas renouveler automatiquement le domaine, mais vous payez à l'avance et le possédez pour l'année. Pour plus d'informations, consultez Enregistrement d'un nouveau domaine dans le Guide du développeur Amazon Route 53.

Étape 1 : créer un compartiment S3

Créez un compartiment destiné à stocker la vidéo d'origine que vous prévoyez de diffuser.

Pour créer un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.

   > **Note**
   >
   > Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste d'Amazon S3 Régions AWS, consultez la section sur les Service AWS points de terminaison dans le Référence générale d'Amazon Web Services.

3. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.

4. Choisissez Créer un compartiment. La page Créer un compartiment s'ouvre.
5. Pour Nom du compartiment, indiquez le nom de votre compartiment, (par exemple, **`tutorial-bucket`**).

   Pour en savoir plus sur les règles d'attribution de noms des compartiments Amazon S3, consultez Règles de dénomination des compartiments à usage général.
6. Pour Région, choisissez l' Région AWS endroit où vous souhaitez que le compartiment réside.

   Si possible, choisissez la région qui est la plus proche de la majorité de vos utilisateurs. Pour en savoir plus sur les régions des compartiments, consultez Présentation des compartiments à usage général.
7. Pour Paramètres de blocage de l'accès public à ce compartiment, conservez les paramètres par défaut (Bloquer tous les accès public est activé).

   Même si l'option Bloquer tout accès public est activée, les spectateurs peuvent toujours accéder à la vidéo mise en ligne via le site CloudFront. Cette fonctionnalité est un avantage majeur de l'utilisation CloudFront pour héberger une vidéo stockée dans S3.

   Nous vous recommandons de laisser tous les paramètres activés, sauf si vous devez en désactiver un ou plusieurs pour votre cas d'utilisation. Pour en savoir plus sur le blocage de l'accès public, consultez Blocage de l'accès public à votre stockage Amazon S3.
8. Pour les paramètres restants, conservez les paramètres par défaut.

   (Facultatif) Si vous souhaitez configurer des paramètres de compartiment supplémentaires pour votre cas d'utilisation particulier, consultez Création d'un bucket à usage général.
9. Choisissez Créer un compartiment.

Étape 2 : charger une vidéo dans le compartiment S3

La procédure suivante explique la manière de télécharger un fichier vidéo dans un compartiment S3 à l'aide de la console. Lorsque vous téléchargez de nombreux fichiers vidéo volumineux sur S3, vous pouvez également utiliser Amazon S3 Transfer Acceleration pour configurer des transferts de fichiers rapides et sécurisés. Transfer Acceleration peut accélérer le chargement de vidéos vers votre compartiment S3 pour le transfert à longue distance de vidéos plus volumineuses. Pour plus d'informations, consultez Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.

Charger un fichier dans le compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments à usage général, choisissez le nom du compartiment que vous avez créé à l'étape 1 (par exemple,**`tutorial-bucket`**) dans lequel télécharger votre fichier.
4. Sous l'onglet Objets de votre compartiment, choisissez Charger.
5. Dans la page Charger, sous Fichiers et dossiers, choisissez Ajouter des fichiers.
6. Choisissez un fichier à charger, puis choisissez Ouvrir.

   Par exemple, vous pouvez charger un fichier vidéo nommé `sample.mp4`.
7. Choisissez Charger.

Étape 3 : créer une identité d'accès à l' CloudFront origine

Pour restreindre l'accès direct à la vidéo depuis votre compartiment S3, créez un CloudFront utilisateur spécial appelé identité d'accès d'origine (OAI). Vous allez associer l'OAI à votre distribution plus tard au cours de ce didacticiel. En utilisant un OAI, vous vous assurez que les spectateurs ne peuvent pas contourner CloudFront et accéder à la vidéo directement depuis le compartiment S3. Seul l' CloudFront OAI peut accéder au fichier dans le compartiment S3. Pour plus d'informations, consultez Restreindre l'accès au contenu Amazon S3 à l'aide d'un OAI dans le manuel Amazon CloudFront Developer Guide.

Pour créer un CloudFront OAI

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans la section Sécurité du volet de navigation de gauche, choisissez Accès à l'origine.
3. Sous l'onglet Identités, choisissez Créer une identité d'accès d'origine.
4. Saisissez un nom (par exemple, **`S3-OAI`**) pour la nouvelle identité d'accès d'origine.
5. Sélectionnez Create (Créer).

Étape 4 : Création d'une CloudFront distribution

Pour l'utiliser CloudFront pour diffuser et distribuer la vidéo dans votre compartiment S3, vous devez créer une CloudFront distribution.

Sous-étapes

- Création d'une CloudFront distribution
- Examiner la politique de compartiment

Création d'une CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Distributions.
3. Choisissez Créer une distribution.
4. Dans la section Origine, pour Domaine d'origine, choisissez le nom de domaine de votre origine S3, qui commence par le nom du compartiment S3 que vous avez créé à l'étape 1 (par exemple, **`tutorial-bucket`**).
5. Pour Accès d'origine, choisissez Identités d'accès existantes.
6. Sous Identité d'accès d'origine, choisissez l'identité d'accès d'origine existante que vous avez créée à l'étape 3 (par exemple, **`S3-OAI`**).
7. Sous Politique de compartiment, choisissez Oui, mettre à jour la politique de compartiment.
8. Dans la section Comportement du cache par défaut, sous Politique du protocole de l'utilisateur, choisissez Rediriger HTTP vers HTTPS.

   Lorsque vous choisissez cette fonction, les requêtes HTTP sont automatiquement redirigées vers HTTPS pour sécuriser votre site web et protéger les données de vos utilisateurs.
9. Pour les autres paramètres de la section Comportement du cache par défaut, conservez les valeurs par défaut.

   (Facultatif) Vous pouvez contrôler la durée pendant laquelle votre fichier reste dans CloudFront le cache avant CloudFront de transmettre une autre demande à votre source. Réduire la durée vous permet de servir des contenus dynamiques. Augmenter la durée signifie que vos utilisateurs obtiennent de meilleures performances parce que vos fichiers sont plus susceptibles d'être servis directement à partir du cache périphérique. Une durée plus longue réduit également

la charge sur votre origine. Pour plus d'informations, consultez Gérer la durée pendant laquelle le contenu reste dans le cache (expiration) dans le manuel Amazon CloudFront Developer Guide.

10. Pour les autres sections, conservez les paramètres restants définis sur les valeurs par défaut.

    Pour plus d'informations sur les différentes options de configuration, consultez la section Valeurs que vous spécifiez lorsque vous créez ou mettez à jour une distribution dans le manuel Amazon CloudFront Developer Guide.

11. En bas de la page, choisissez Créer une distribution.
12. Dans l'onglet Général de votre CloudFront distribution, sous Détails, la valeur de la colonne Dernière modification de votre distribution passe de Déploiement à l'horodatage de la dernière modification de la distribution. Ce processus prend généralement quelques minutes.

Examiner la politique de compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste des compartiments, choisissez le nom du compartiment que vous avez utilisé précédemment comme origine de votre CloudFront distribution (par exemple,**`tutorial-bucket`**).
4. Sélectionnez l'onglet Autorisations.
5. Dans la boîte de dialogue Politique de compartiment, confirmez que vous voyez une instruction similaire à ce qui suit s'affiche dans le texte de la politique de compartiment :

```
{
    "Version": "2008-10-17",
    "Id": "PolicyForCloudFrontPrivateContent",
    "Statement": [
        {
            "Sid": "1",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::cloudfront:user/CloudFront Origin Access
 Identity EH1HDMB1FH2TC"
            },
            "Action": "s3:GetObject",
            "Resource": "arn:aws:s3:::tutorial-bucket/*"
        }
```

```
    ]
}
```

Il s'agit de la déclaration que votre CloudFront distribution a ajoutée à votre politique de compartiment lorsque vous avez choisi Oui, mettez à jour la politique de compartiment plus tôt.

Cette mise à jour de la politique de compartiment indique que vous avez correctement configuré la CloudFront distribution pour restreindre l'accès au compartiment S3. En raison de cette restriction, les objets du compartiment ne sont accessibles que par le biais de votre CloudFront distribution.

Étape 5 : Accédez à la vidéo via la CloudFront distribution

CloudFront Vous pouvez désormais diffuser la vidéo stockée dans votre compartiment S3. Pour accéder à votre vidéo CloudFront, vous devez associer le nom de votre domaine de CloudFront distribution au chemin d'accès à la vidéo dans le compartiment S3.

Pour créer une URL vers la vidéo S3 à l'aide du nom CloudFront de domaine de distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le panneau de navigation de gauche, choisissez Distributions.
3. Pour obtenir le nom de domaine de distribution, procédez comme suit :
   a. Dans la colonne Origins, recherchez la CloudFront distribution correcte en recherchant son nom d'origine, qui commence par le compartiment S3 que vous avez créé à l'étape 1 (par exemple,**`tutorial-bucket`**).
   b. Après avoir trouvé la distribution dans la liste, élargissez la colonne Nom de domaine pour copier la valeur du nom de domaine de votre CloudFront distribution.
4. Dans un nouvel onglet du navigateur, collez le nom de domaine de distribution que vous avez copiés.
5. Retournez à l'onglet de navigateur précédent et ouvrez la console S3 à l'adresse https://console.aws.amazon.com/s3/.
6. Dans le panneau de navigation de gauche, choisissez Compartiments.
7. Dans la liste Compartiments, choisissez le nom du compartiment que vous avez créé à l'étape 1 (par exemple, **`tutorial-bucket`**).

8. Dans la liste Objets, choisissez le nom de la vidéo que vous avez téléchargée à l'étape 2 (par exemple, `sample.mp4`).
9. Sur la page détaillée de l'objet, dans la section Présentation de l'objet, copiez la valeur de la clé. Cette valeur correspond au chemin d'accès à l'objet vidéo chargé dans le compartiment S3.
10. Revenez à l'onglet du navigateur dans lequel vous avez précédemment collé le nom de domaine de distribution, saisissez une barre oblique (**/**) après le nom de domaine de distribution, puis collez le chemin d'accès à la vidéo que vous avez copiée précédemment (par exemple, `sample.mp4`).

    Votre vidéo S3 est désormais accessible CloudFront au public et hébergée via une URL similaire à la suivante :

    ```
    https://CloudFront distribution domain name/Path to the S3 video
    ```

    Remplacez *`CloudFront distribution domain name`* et *`Path to the S3 video`* par les valeurs appropriées. Voici un exemple d'URL : **`https://d111111abcdef8.cloudfront.net/sample.mp4`**.

Étape 6 : configurer votre CloudFront distribution pour utiliser votre nom de domaine personnalisé

Pour utiliser votre propre nom de domaine au lieu du nom de CloudFront domaine indiqué dans l'URL pour accéder à la vidéo S3, ajoutez un autre nom de domaine à votre CloudFront distribution.

Sous-étapes

- Demander un certificat SSL
- Ajoutez le nom de domaine alternatif à votre CloudFront distribution
- Créez un enregistrement DNS pour acheminer le trafic de votre nom de domaine alternatif vers le nom de domaine de votre CloudFront distribution
- Vérifiez si cette option IPv6 est activée pour votre distribution et créez un autre enregistrement DNS si nécessaire

Demander un certificat SSL

Pour permettre à vos spectateurs d'utiliser le protocole HTTPS et votre nom de domaine personnalisé dans l'URL de votre diffusion vidéo, utilisez AWS Certificate Manager (ACM) pour demander un

certificat SSL (Secure Sockets Layer). Le certificat SSL établit une connexion réseau chiffrée au site web.

1. Connectez-vous à la console ACM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/acm/l'adresse.
2. Si la page d'introduction s'affiche, sous Allocation de certificats, choisissez Mise en route.
3. Dans la page Request a certificate (Demander un certificat), choisissez Request a public certificate (Demander un certificat public) et Request a certificate (Demander un certificat).
4. Dans la page Add domain names (Ajouter des noms de domaine), saisissez le nom de domaine complet (FQDN) du site que vous souhaitez sécuriser à l'aide d'un certificat SSL/TLS. Vous pouvez utiliser un astérisque (*) pour créer un certificat générique qui protègera plusieurs noms de site du même domaine. Plus précisément, dans ce didacticiel, saisissez ***** et le nom de domaine personnalisé que vous avez configuré dans Prerequisites (Conditions préalables). Pour cet exemple, saisissez **`*.example.com`**, puis choisissez Next (Suivant).

   Pour plus d'informations, consultez Demander un certificat public ACM (console) dans le guide de l'utilisateur AWS Certificate Manager .
5. Sur la page Sélectionner une méthode de validation, choisissez validation du DNS. Ensuite, choisissez Suivant.

   Si vous êtes en mesure de modifier la configuration DNS, nous vous recommandons d'utiliser la validation de domaine DNS plutôt que la validation par e-mail. La validation du DNS présente plusieurs avantages par rapport à la validation par e-mail. Pour plus d'informations, consultez Option 1 : validation DNS dans le Guide de l'utilisateur AWS Certificate Manager .
6. (Facultatif) Étiquetez votre certificat à l'aide de métadonnées sur la page Ajouter des balises.
7. Choisissez Examiner.
8. Sur la page Vérification, vérifiez que les informations sous Domain name (Nom de domaine) et Validation method (Méthode de validation) sont correctes. Ensuite, choisissez Confirmer et demander.

   La page Validation indique que votre demande est en cours de traitement et que les domaines de certificat sont en cours de validation. Le certificat en attente de validation est dans l'état En attente de validation.
9. Dans la page Validation, appuyez sur la flèche vers le bas à gauche de votre nom de domaine personnalisé, puis choisissez Create record in Route 53 (Créer un registre dans Route 53) pour valider la propriété du domaine via le DNS.

Cela ajoute un enregistrement CNAME fourni par AWS Certificate Manager à votre configuration DNS.

10. Dans la boîte de dialogue Créer un enregistrement dans Route 53, choisissez Créer.

    La page Validation devrait afficher une notification d'état Success (Réussite) en bas.

11. Choisissez Continuer pour afficher la page de la liste des certificats.

    L'état de votre nouveau certificat passera de Pending validation (En attente de validation) à Issued (Émis) dans les 30 minutes.

Ajoutez le nom de domaine alternatif à votre CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, choisissez Distributions.
3. Choisissez l'ID de la distribution que vous avez créée à l'étape 4.
4. Sur la page General (Général), accédez à l'onglet Settings (Paramètres) et choisissez Edit (Modifier).
5. Sur la page Modifier les paramètres, pour Nom de domaine alternatif (CNAME) - facultatif, choisissez Ajouter un élément pour ajouter les noms de domaine personnalisés que vous souhaitez utiliser dans l'URL de la vidéo S3 diffusée par cette CloudFront distribution.

   Dans ce didacticiel, par exemple, si vous souhaitez acheminer le trafic d'un sous-domaine, tel que `www.example.com`, saisissez le nom de sous-domaine (`www`) avec le nom de domaine (`example.com`). Plus précisément, saisissez **`www.example.com`**.

   > **Note**
   >
   > Le nom de domaine alternatif (CNAME) que vous ajoutez doit être couvert par le certificat SSL que vous avez précédemment attaché à votre CloudFront distribution.

6. Pour Custom SSL certificate - optional (Certificat SSL personnalisé - facultatif), choisissez le certificat SSL que vous avez demandé précédemment (par exemple, **`*.example.com`**).

> **Note**
>
> Si le certificat SSL ne s'affiche pas immédiatement après l'avoir demandé, patientez 30 minutes, puis actualisez la liste jusqu'à ce que le certificat SSL soit disponible afin que vous puissiez le sélectionner.

7. Conservez les paramètres restants définis sur les valeurs par défaut. Sélectionnez Enregistrer les modifications.
8. Dans l'onglet General (Généra)l de la distribution, attendez que la valeur de Last modified (Dernière modification) passe de Deploying (Déploiement) à l'horodatage du moment où la distribution a été modifiée pour la dernière fois.

Créez un enregistrement DNS pour acheminer le trafic de votre nom de domaine alternatif vers le nom de domaine de votre CloudFront distribution

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet gauche de navigation, choisissez Hosted zones (Zones hébergées).
3. Dans la page Zones hébergées, choisissez le nom de la zone hébergée que Route 53 a créée pour vous dans les conditions préalables (par exemple, **`example.com`**).
4. Choisissez Create record (Créer un registre), puis utilisez la méthode Quick create record (Création rapide de registre).
5. Pour Nom de l'enregistrement, conservez la même valeur que le nom de domaine alternatif de la CloudFront distribution que vous avez ajouté précédemment.

   Dans ce didacticiel, pour acheminer le trafic vers un sous-domaine, tel que `www.example.com`, saisissez le nom de sous-domaine sans le nom de domaine. Par exemple, saisissez uniquement **`www`** dans le champ de texte avant votre nom de domaine personnalisé.
6. Pour Type d'enregistrement, choisissez A - Achemine le trafic vers une IPv4 adresse et certaines AWS ressources.
7. Pour Value (Valeur), choisissez Alias pour activer la ressource Alias.
8. Sous Acheminer le trafic vers, choisissez Alias vers la CloudFront distribution dans la liste déroulante.

9. Dans la zone de recherche intitulée Choisir une distribution, choisissez le nom de domaine de la CloudFront distribution que vous avez créée à l'étape 4.

   Pour trouver le nom de domaine de votre CloudFront distribution, procédez comme suit :

   a. Dans un nouvel onglet du navigateur, connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v3/home.
   b. Dans le volet de navigation de gauche, choisissez Distributions.
   c. Dans la colonne Origins, recherchez la CloudFront distribution correcte en recherchant son nom d'origine, qui commence par le compartiment S3 que vous avez créé à l'étape 1 (par exemple,**`tutorial-bucket`**).
   d. Après avoir trouvé la distribution dans la liste, élargissez la colonne Nom de domaine pour voir la valeur du nom de domaine de votre CloudFront distribution.

10. Sur la page Create record (Création de registre) de la console Route 53, conservez les valeurs par défaut pour les paramètres restants.
11. Choisissez Créer des enregistrements.

Vérifiez si cette option IPv6 est activée pour votre distribution et créez un autre enregistrement DNS si nécessaire

Si cette option IPv6 est activée pour votre distribution, vous devez créer un autre enregistrement DNS.

1. Pour vérifier si cette option IPv6 est activée pour votre distribution, procédez comme suit :

   a. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
   b. Dans le volet de navigation de gauche, choisissez Distributions.
   c. Choisissez l'ID de la CloudFront distribution que vous avez créée à l'étape 4.
   d. Dans l'onglet Général, sous Paramètres, vérifiez si le paramètre IPv6est défini sur Activé.

      Si cette option IPv6 est activée pour votre distribution, vous devez créer un autre enregistrement DNS.

2. Si cette option IPv6 est activée pour votre distribution, procédez comme suit pour créer un enregistrement DNS :

a. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.

b. Dans le volet gauche de navigation, choisissez Hosted zones (Zones hébergées).

c. Dans la page Zones hébergées, choisissez le nom de la zone hébergée que Route 53 a créée pour vous dans les conditions préalables (par exemple, **`example.com`**).

d. Choisissez Create record (Créer un registre), puis utilisez la méthode Quick create record (Création rapide de registre).

e. Pour Nom de l'enregistrement, dans le champ de texte situé avant votre nom de domaine personnalisé, saisissez la même valeur que celle que vous avez saisie lors de la création de l'enregistrement IPv4 DNS plus tôt. Par exemple, dans ce didacticiel, pour acheminer le trafic pour le sous-domaine `www.example.com`, saisissez uniquement **`www`**.

f. Pour Type d'enregistrement, choisissez AAAA - Achemine le trafic vers une IPv6 adresse et certaines AWS ressources.

g. Pour Value (Valeur), choisissez Alias pour activer la ressource Alias.

h. Sous Acheminer le trafic vers, choisissez Alias vers la CloudFront distribution dans la liste déroulante.

i. Dans la zone de recherche intitulée Choisir une distribution, choisissez le nom de domaine de la CloudFront distribution que vous avez créée à l'étape 4.

j. Pour les paramètres restants, conservez les paramètres par défaut.

k. Choisissez Créer des enregistrements.

Étape 7 : Accédez à la vidéo S3 via la CloudFront distribution avec le nom de domaine personnalisé

Pour accéder à la vidéo S3 à l'aide de l'URL personnalisée, vous devez associer votre autre nom de domaine au chemin d'accès à la vidéo dans le compartiment S3.

Pour créer une URL personnalisée permettant d'accéder à la vidéo S3 via la CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, choisissez Distributions.
3. Pour obtenir le nom de domaine alternatif de votre CloudFront distribution, procédez comme suit :

a. Dans la colonne Origins, recherchez la CloudFront distribution correcte en recherchant son nom d'origine, qui commence par le nom du compartiment S3 que vous avez créé à l'étape 1 (par exemple,**`tutorial-bucket`**).

b. Après avoir trouvé la distribution dans la liste, élargissez la colonne Noms de domaine alternatifs pour copier la valeur du nom de domaine alternatif de votre CloudFront distribution.

4. Dans un nouvel onglet du navigateur, collez le nom de domaine alternatif de la CloudFront distribution.
5. Retournez à l'onglet de navigateur précédent et ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
6. Recherchez le chemin d'accès à votre vidéo S3, comme expliqué à l'étape 5.
7. Retournez à l'onglet du navigateur où vous avez précédemment collé le nom de domaine alternatif, saisissez une barre oblique (**/**) et collez le chemin d'accès à votre vidéo S3 (par exemple, `sample.mp4`).

   Votre vidéo S3 est désormais accessible au public et hébergée via CloudFront une URL personnalisée qui ressemble à ce qui suit :

   ```
   https://CloudFront distribution alternate domain name/Path to the S3 video
   ```

   Remplacez *`CloudFront distribution alternate domain name`* et *`Path to the S3 video`* par les valeurs appropriées. Voici un exemple d'URL : **`https://www.example.com/sample.mp4`**.

(Facultatif) Étape 8 : Afficher les données relatives aux demandes reçues par votre CloudFront distribution

Pour consulter les données relatives aux demandes reçues par votre CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, sous Rapports et analytique, choisissez les rapports dans la console parmi Statistiques du cache, Objets populaires, Principaux référents, Utilisation et Utilisateurs.

Vous pouvez filtrer le tableau de bord de chaque rapport. Pour plus d'informations, consultez la section CloudFront Rapports de la console dans le manuel Amazon CloudFront Developer Guide.

3. Pour filtrer les données, choisissez l'ID de la CloudFront distribution que vous avez créée à l'étape 4.

Étape 9 : nettoyer

Si vous avez hébergé une vidéo S3 en streaming en utilisant CloudFront Route 53 uniquement à titre d'exercice d'apprentissage, supprimez les AWS ressources que vous avez allouées afin de ne plus accumuler de frais.

> **Note**
>
> Lorsque vous enregistrez un domaine, cela coûte immédiatement de l'argent et c'est irréversible. Vous pouvez choisir de ne pas renouveler automatiquement le domaine, mais vous payez à l'avance et le possédez pour l'année. Pour plus d'informations, consultez Enregistrement d'un nouveau domaine dans le Guide du développeur Amazon Route 53.

Sous-étapes

- Supprimer la CloudFront distribution
- Suppression du registre DNS
- Supprimer la zone hébergée publique de votre domaine personnalisé
- Supprimer le nom de domaine personnalisé de Route 53
- Supprimer la vidéo d'origine dans le compartiment source S3
- Supprimer le compartiment source S3

Supprimer la CloudFront distribution

1. Connectez-vous à la CloudFront console AWS Management Console et ouvrez-la à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Dans le volet de navigation de gauche, choisissez Distributions.

3. Dans la colonne Origins, recherchez la CloudFront distribution correcte en recherchant son nom d'origine, qui commence par le nom du compartiment S3 que vous avez créé à l'étape 1 (par exemple,**`tutorial-bucket`**).
4. Pour supprimer la CloudFront distribution, vous devez d'abord la désactiver.
   - Si la valeur de la colonne Status (État) est Enabled (Activé) et si la valeur Last modified (Dernière modification) est l'horodatage au moment de la dernière modification de la distribution, continuez à désactiver la distribution avant de la supprimer.
   - Si la valeur de Status (État) est Enabled (Activé) et si la valeur Last modified (Dernière modification) est Deploying (Déploiement), attendez jusqu'à ce que la valeur de Status (État) passe à l'horodatage du moment où la distribution a été modifiée pour la dernière fois. Continuez ensuite pour désactiver la distribution avant de la supprimer.
5. Pour désactiver la CloudFront distribution, procédez comme suit :
   a. Dans la liste Distributions, cochez la case en regard de l'ID de la distribution que vous souhaitez supprimer.
   b. Pour désactiver la distribution, choisissez Désactiver, puis Désactiver pour confirmer.

      Si vous désactivez une distribution associée à un autre nom de domaine, elle CloudFront cesse d'accepter du trafic pour ce nom de domaine (par exemple`www.example.com`), même si une autre distribution possède un nom de domaine alternatif avec un caractère générique (`*`) correspondant au même domaine (tel que`*.example.com`).
   c. La valeur de la colonne État passe immédiatement sur Désactivé. Attendez que la valeur Last modified (Dernière modification) passe de Deploying (Déploiement) à l'horodatage du moment où la distribution a été modifiée pour la dernière fois.

      Comme cette modification CloudFront doit être étendue à tous les emplacements périphériques, cela peut prendre quelques minutes avant que la mise à jour ne soit terminée et que l'option Supprimer soit disponible pour vous permettre de supprimer la distribution.
6. Pour supprimer la distribution désactivée, procédez comme suit :
   a. Cochez la case en regard de l'ID de la distribution que vous souhaitez supprimer.
   b. Choisissez Supprimer, puis Supprimer pour confirmer.

Suppression du registre DNS

Si vous souhaitez supprimer la zone hébergée publique du domaine (y compris le registre DNS), consultez Supprimer la zone hébergée publique de votre domaine personnalisé dans le Guide du développeur Amazon Route 53. Si vous souhaitez seulement supprimer le registre DNS créé à l'étape 6, procédez comme suit :

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet gauche de navigation, choisissez Hosted zones (Zones hébergées).
3. Dans la page Zones hébergées, choisissez le nom de la zone hébergée que Route 53 a créée pour vous dans les conditions préalables (par exemple, **`example.com`**).
4. Dans la liste des registres, cochez la case à côté des registres que vous voulez supprimer (les registres que vous avez créés à l'étape 6).

   > **Note**
   >
   > Vous ne pouvez pas supprimer les registres dont la valeur est NS ou SOA pour le champ Type.

5. Choisissez Supprimer un jeu de registres.
6. Pour confirmer la suppression, choisissez Supprimer.

   La propagation de vos registres modifiés sur les serveurs DNS Route 53 n'est pas immédiate. À l'heure actuelle, le seul moyen de vérifier que vos modifications se sont propagées consiste à utiliser l'action GetChange API. Les modifications se propagent généralement sur tous les serveurs de Route 53 en 60 secondes.

Supprimer la zone hébergée publique de votre domaine personnalisé

> **Warning**
>
> Si vous souhaitez conserver l'enregistrement de votre domaine, mais que vous souhaitez arrêter d'acheminer le trafic Internet vers votre site web ou votre application Web, nous vous recommandons de supprimer les registres dans la zone hébergée (comme expliqué dans la section précédente) au lieu de supprimer la zone hébergée.

Si vous supprimez une zone hébergée, quelqu'un d'autre peut utiliser le domaine et acheminer le trafic vers ses propres ressources à l'aide de votre nom de domaine.
En outre, si vous supprimez une zone hébergée, vous ne pourrez pas annuler cette suppression. Vous devrez créer une nouvelle zone hébergée et mettre à jour les serveurs de noms pour l'enregistrement de votre domaine, ce qui peut demander jusqu'à 48 heures pour prendre effet.
Si vous ne voulez pas que le domaine soit disponible sur Internet, vous pouvez d'abord transférer votre service DNS vers un service DNS gratuit, puis supprimer la zone hébergée Route 53. Cela évitera les requêtes DNS futures d'être mal acheminées.

1. Si le domaine est enregistré auprès de Route 53, consultez Ajout ou modification de serveurs de noms et de registres de type Glue pour un domaine dans le Guide du développeur Amazon Route 53 pour savoir comment remplacer des serveurs de noms Route 53 par des serveurs de noms pour le nouveau service DNS.
2. Si le domaine est enregistré auprès d'un autre bureau d'enregistrement, utilisez la méthode fournie par le bureau d'enregistrement pour changer les serveurs de noms du domaine.

> **Note**
>
> Si vous supprimez une zone hébergée pour un sous-domaine (`www.example.com`), vous n'avez pas besoin de changer les serveurs de noms du domaine (`example.com`).

1. Connectez-vous à la console Route 53 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/route53/.
2. Dans le volet gauche de navigation, choisissez Hosted zones (Zones hébergées).
3. Dans la page Zones hébergées, choisissez la ligne de la zone hébergée que vous souhaitez supprimer.
4. Sur l'onglet Registres de votre zone hébergée, vérifiez que la zone hébergée que vous souhaitez supprimer contient uniquement un NS et un registre SOA.

   Si elle contient d'autres registres, supprimez-les en premier lieu.

Si vous avez créé des registres NS pour des sous-domaines dans la zone hébergée, supprimez également ces registres.

5. Sur l'onglet Signature DNSSEC de votre zone hébergée, désactivez la signature DNNSSEC si elle était activée. Pour plus d'informations, consultez Désactivation de la signature DNSSEC dans le Guide du développeur Amazon Route 53.
6. En haut de la page des détails de la zone hébergée, choisissez Delete zone (Supprimer une zone).
7. Saisissez **`delete`** pour confirmer la suppression, puis choisissez Supprimer.

Supprimer le nom de domaine personnalisé de Route 53

Pour la plupart des domaines de premier niveau (TLDs), vous pouvez supprimer l'enregistrement si vous ne le souhaitez plus. Si vous supprimez un enregistrement de nom de domaine sur Route 53 avant l'expiration prévue de l'enregistrement, les frais d'enregistrement AWS ne sont pas remboursés. Pour plus d'informations, consultez Suppression d'un enregistrement de nom de domaine dans le Guide du développeur Amazon Route 53.

> **Important**
>
> Si vous souhaitez transférer le domaine entre Comptes AWS ou transférer le domaine vers un autre bureau d'enregistrement, ne supprimez pas le domaine et attendez-vous à le réenregistrer immédiatement. Consultez plutôt la documentation pertinente dans le Guide du développeur Amazon Route 53 :
>
> - Transférer un domaine vers un autre Compte AWS
> - Transfert d'un domaine depuis Amazon Route 53 vers un autre bureau d'enregistrement

Supprimer la vidéo d'origine dans le compartiment source S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Bucket name (Nom du compartiment), choisissez le nom du compartiment dans lequel vous avez téléchargé la vidéo à l'étape 2 (par exemple, **`tutorial-bucket`**).

4. Sur l'onglet Objects (Objets), cochez la case située en regard du nom de l'objet que vous souhaitez supprimer (par exemple, `sample.mp4`).
5. Sélectionnez Delete (Supprimer).
6. Sous Supprimer définitivement les objets ?, saisissez **`permanently delete`** pour confirmer que vous souhaitez supprimer cet objet.
7. Choisissez Supprimer les objets.

Supprimer le compartiment source S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Buckets (Compartiments), choisissez le bouton d'option en regard du nom du compartiment que vous avez créé à l'étape 1 (par exemple, **`tutorial-bucket`**).
4. Sélectionnez Delete (Supprimer).
5. Dans la page Supprimer le compartiment, confirmez que vous souhaitez supprimer le compartiment en saisissant le nom de ce dernier dans le champ de texte, puis choisissez Supprimer le compartiment.

Étapes suivantes

Après avoir terminé ce didacticiel, vous pouvez explorer plus en détail les cas d'utilisation connexes suivants :

- Transcodez les vidéos S3 dans les formats de streaming requis par un téléviseur ou un appareil connecté en particulier avant de les héberger dans une CloudFront distribution.

  Pour utiliser Amazon S3 Batch Operations AWS Lambda et AWS Elemental MediaConvert pour transcoder par lots une collection de vidéos vers différents formats de sortie, consultez. Didacticiel : transcodage par lot de vidéos avec les opérations par lot S3
- Hébergez d'autres objets stockés dans S3, tels que des images, du son, des animations, des feuilles de style, du HTML JavaScript, des applications React, etc., à l'aide CloudFront de Route 53.

  Consultez, par exemple, Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53 et Accélérez votre site Web avec Amazon CloudFront.

- Utiliser Amazon S3 Transfer Acceleration pour configurer des transferts de fichiers rapides et sécurisés. Transfer Acceleration peut accélérer le chargement de vidéos vers votre compartiment S3 pour le transfert à longue distance de vidéos plus volumineuses. L'accélération des transferts améliore les performances de transfert en acheminant le trafic via les emplacements périphériques répartis CloudFront dans le monde entier et via AWS les réseaux principaux. Elle utilise également des optimisations de protocole réseau. Pour de plus amples informations, veuillez consulter Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.

Didacticiel : configuration d'un site web statique sur Amazon S3

> **Important**
>
> Amazon S3 applique désormais le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) comme niveau de base du chiffrement pour chaque compartiment d'Amazon S3. À partir du 5 janvier 2023, tous les nouveaux chargements d'objets sur Amazon S3 sont automatiquement chiffrés, sans coût supplémentaire et sans impact sur les performances. L'état du chiffrement automatique pour la configuration de chiffrement par défaut du compartiment S3 et pour le téléchargement de nouveaux objets est disponible dans AWS CloudTrail les journaux, S3 Inventory, S3 Storage Lens, la console Amazon S3 et sous forme d'en-tête de réponse d'API Amazon S3 supplémentaire dans le AWS Command Line Interface et AWS SDKs. Pour plus d'informations, consultez la FAQ sur le chiffrement par défaut.

Vous pouvez configurer un compartiment Amazon S3 afin qu'il fonctionne comme un site web. Cet exemple explique les différentes étapes d'hébergement d'un site web sur Amazon S3.

> **Important**
>
> Le didacticiel suivant nécessite la désactivation du blocage de l'accès public. Nous vous recommandons de maintenir activé le blocage de l'accès public. Si vous souhaitez conserver les quatre paramètres de blocage de l'accès public activés et héberger un site Web statique, vous pouvez utiliser le contrôle CloudFront d'accès d'origine (OAC) d'Amazon. Amazon CloudFront fournit les fonctionnalités requises pour configurer un site Web statique sécurisé. Les sites Web statiques Amazon S3 prennent uniquement en charge les points de terminaison HTTP. Amazon CloudFront utilise le stockage durable d'Amazon S3 tout

en fournissant des en-têtes de sécurité supplémentaires, tels que HTTPS. HTTPS accroît la sécurité en chiffrant une demande HTTP normale et en offrant une protection contre les cyberattaques courantes. Pour plus d'informations, consultez Getting started with a secure static website in the Amazon CloudFront Developer Guide.

Rubriques

- Étape 1 : créer un compartiment
- Étape 2 : activer l'hébergement de site web statique
- Étape 3 : modifier les paramètres de blocage de l'accès public
- Étape 4 : ajouter une politique de compartiment visant à rendre disponible publiquement le contenu de votre compartiment
- Étape 5 : configurer un document d'index
- Étape 6 : configurer un document d'erreur
- Étape 7 : tester le point de terminaison de votre site web
- Étape 8 : nettoyer

Étape 1 : créer un compartiment

Les instructions ci-dessous fournissent une vue d'ensemble de la façon de créer vos compartiments pour l'hébergement de site web. Pour obtenir des step-by-step instructions détaillées sur la création d'un bucket, consultezCréation d'un bucket à usage général.

Pour créer un compartiment

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez Créer un compartiment.
3. Saisissez le Nom du compartiment (par exemple **`example.com`**).
4. Choisissez la Région dans laquelle vous souhaitez créer le compartiment.

   Choisissez une Région proche de vous sur le plan géographique afin de limiter la latence et les coûts, ou de répondre aux exigences réglementaires. C'est la Région que vous choisissez qui détermine votre point de terminaison de site web Amazon S3. Pour plus d'informations, consultez Points de terminaison de sites web.

5. Pour accepter les paramètres par défaut et créer le compartiment, choisissez Créer.

Étape 2 : activer l'hébergement de site web statique

Après avoir créé un compartiment, vous pouvez activer l'hébergement de site web statique pour votre compartiment. Vous pouvez créer un compartiment ou utiliser un compartiment existant.

Pour activer l'hébergement de site Web statique

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer l'hébergement statique de sites Web.
4. Choisissez Propriétés.
5. Sous Static website hosting (Hébergement de site Web statique), choisissez Edit (Modifier).
6. Choisissez Utiliser ce compartiment pour héberger un site Web.
7. Sous Static website hosting (Hébergement de site web statique), choisissez Enable (Activer).
8. Dans Index document (Document d'index), entrez le nom du document d'index, généralement `index.html`.

   Le nom du document d'index est sensible à la casse et doit correspondre exactement au nom de fichier du document d'index HTML que vous prévoyez de charger dans votre compartiment S3. Lorsque vous configurez un compartiment pour l'hébergement d'un site web, vous devez indiquer un document d'index. Amazon S3 renvoie ce document d'index lorsque des demandes sont faites dans le domaine racine ou dans n'importe quel sous-dossier. Pour plus d'informations, consultez Configuration d'un document d'index.
9. Pour fournir votre propre document d'erreur personnalisé pour les erreurs de classe 4XX, entrez le nom du fichier du document d'erreur personnalisé dans Document d'erreur.

   Le nom du document d'erreur est sensible à la casse et doit correspondre exactement au nom de fichier du document d'erreur HTML que vous prévoyez de charger dans votre compartiment S3. Si vous ne spécifiez pas de document d'erreur personnalisé et qu'une erreur se produit, Amazon S3 renvoie un document d'erreur HTML par défaut. Pour plus d'informations, consultez Configuration d'un document d'erreur personnalisé.

10. (Facultatif) Si vous souhaitez spécifier des règles de redirection avancées, décrivez les règles à l'aide du langage JSON dans Redirection rules (Règles de redirection).

    Par exemple, vous pouvez acheminer les demandes de façon conditionnelle en fonction des noms ou préfixes de clés d'objets dans la demande. Pour plus d'informations, consultez Configurer des règles de redirection pour utiliser des redirections conditionnelles avancées.
11. Choisissez Enregistrer les modifications.

    Amazon S3 permet l'hébergement de site web statique pour votre compartiment. Au bas de la page, sous Static website hosting (Hébergement de site Web statique), vous voyez le point de terminaison du site web pour votre compartiment.
12. Sous Static website hosting (Hébergement de site Web statique), notez la valeur de Endpoint (Point de terminaison).

    Endpoint (Point de terminaison) correspond au point de terminaison du site web Amazon S3 de votre compartiment. Une fois que vous avez terminé de configurer votre compartiment en tant que site Web statique, vous pouvez utiliser ce point de terminaison pour tester votre site Web.

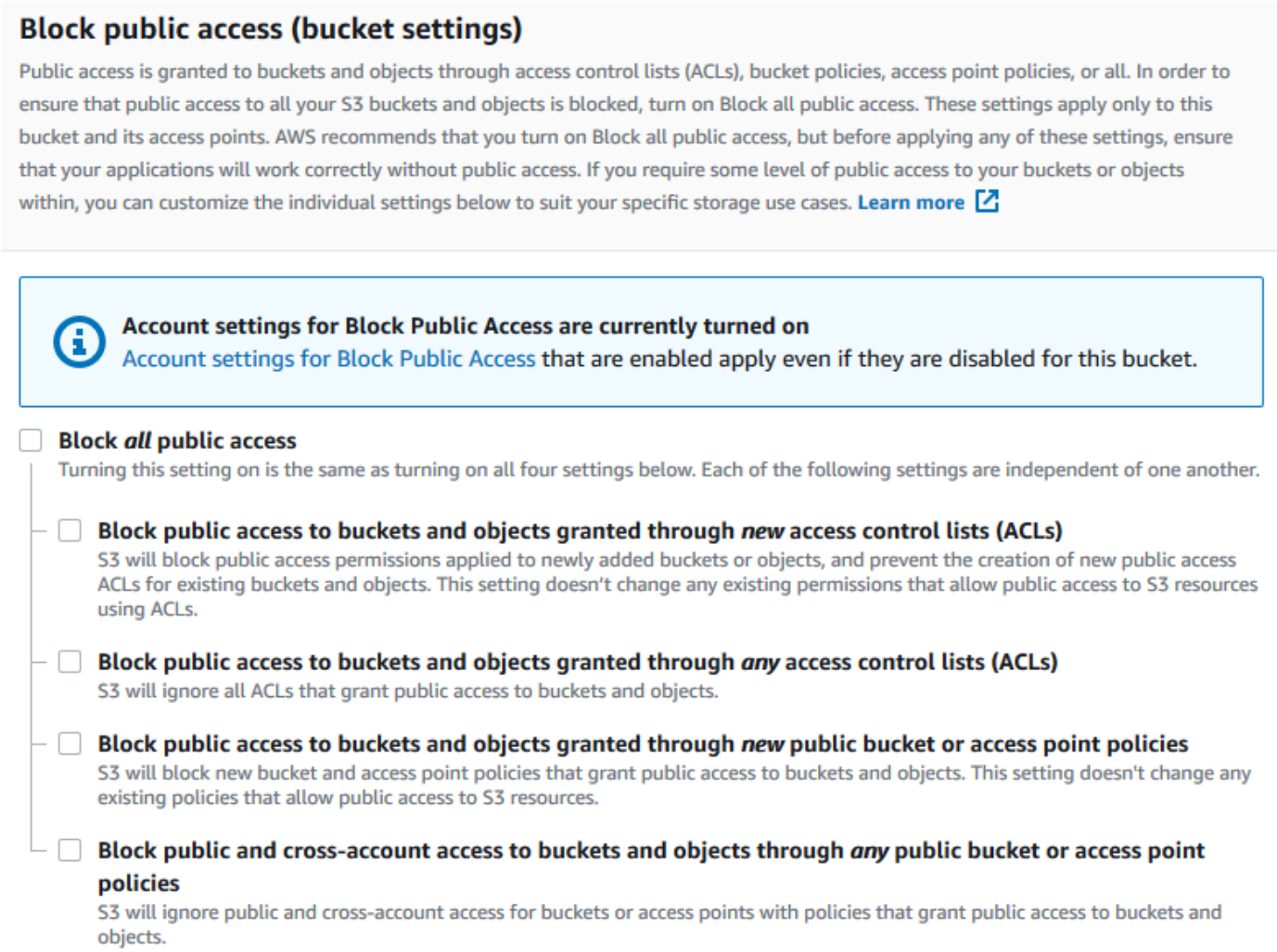
Étape 3 : modifier les paramètres de blocage de l'accès public

Par défaut, Amazon S3 bloque l'accès public à votre compte et à vos compartiments. Si vous souhaitez utiliser un compartiment pour héberger un site web statique, vous pouvez utiliser ces étapes pour modifier vos paramètres de blocage de l'accès public.

> **Warning**
>
> Avant de suivre ces étapes, passez en revue Blocage de l'accès public à votre stockage Amazon S3 pour vous assurer que vous comprenez et acceptez les risques liés à l'autorisation de l'accès public. Lorsque vous désactivez les paramètres de blocage de l'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tous les accès publics à vos compartiments.

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le nom du compartiment que vous avez configuré en tant que site web statique.
3. Choisissez Permissions.

4. Sous Block public access (bucket settings) (Bloquer l'accès public (paramètres de compartiment)), choisissez Edit (Modifier).
5. Décochez Bloquer tous les accès publics et sélectionnez Enregistrer les modifications.



Amazon S3 désactive les paramètres de blocage de l'accès public pour votre compartiment. Pour créer un site Web public statique, vous devrez peut-être aussi modifier les paramètres de blocage de l'accès public de votre compte avant d'ajouter une politique de compartiment. Si les paramètres de blocage de l'accès public pour votre compte sont actuellement activés, une note s'affiche sous Bloquer l'accès public (paramètres de compartiment).

Étape 4 : ajouter une politique de compartiment visant à rendre disponible publiquement le contenu de votre compartiment

Après avoir modifié les paramètres de blocage de l'accès public S3, vous devez ajouter une stratégie de compartiment pour accorder un accès public en lecture à votre compartiment. Lorsque vous accordez un accès public en lecture, tout le monde sur Internet peut accéder à votre compartiment.

> **Important**
>
> La stratégie suivante est uniquement un exemple et autorise un accès complet au contenu de votre compartiment. Avant d'effectuer cette étape, consultez Comment assurer la sécurité des fichiers de mon compartiment Amazon S3 ?, pour vous assurer que vous comprenez les bonnes pratiques pour sécuriser les fichiers dans votre compartiment S3 et les risques liés à l'octroi d'un accès public.

1. Dans Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Permissions.
3. Sous Politique de compartiment, choisissez Modifier.
4. Pour accorder l'accès public en lecture à votre site web, copiez la politique de compartiment suivante et collez-la dans l'Éditeur de politique de compartiment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. Mettez à jour `Resource` pour inclure le nom de votre compartiment.

Dans l'exemple de politique de compartiment précédent, *Bucket-Name* il s'agit d'un espace réservé pour le nom du compartiment. Pour utiliser cette politique de compartiment avec votre propre compartiment, vous devez mettre à jour ce nom pour qu'il corresponde à celui de votre compartiment.

6. Sélectionnez Enregistrer les modifications.

   Un message s'affiche indiquant que la politique de compartiment a été ajoutée avec succès.

   Si une erreur indique `Policy has invalid resource`, confirmez que le nom du compartiment dans la politique de compartiment correspond au nom de votre compartiment. Pour plus d'informations sur l'ajout d'une politique de compartiment, consultez Comment ajouter une politique de compartiment S3 ?

   Si vous recevez un message d'erreur et que vous ne pouvez pas enregistrer la stratégie de compartiment, vérifiez les paramètres de blocage de l'accès public de votre compte et de votre compartiment pour confirmer que vous autorisez l'accès public au compartiment.

Étape 5 : configurer un document d'index

Lorsque vous activez l'hébergement de site web statique pour votre compartiment, vous saisissez le nom du document d'index (par exemple, **`index.html`**). Après avoir activé l'hébergement de site web statique pour le compartiment, vous téléchargez un fichier HTML avec le nom du document de cet index dans votre compartiment.

Pour configurer le document d'index

1. Créez un fichier `index.html`.

   Si vous n'avez pas de ficher `index.html`, vous pouvez utiliser le code HTML suivant pour en créer un :

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
    <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
```

```
</html>
```

2. Enregistrez le fichier d'index au niveau local.

   Le nom du fichier du document d'index doit correspondre exactement au nom du document d'index que vous saisissez dans la boîte de dialogue Hébergement de site Web statique. Le nom du document d'index est sensible à la casse. Par exemple, si vous saisissez `index.html` pour le nom du Document d'index dans la boîte de dialogue Hébergement de site Web statique, le nom du fichier de votre document d'index doit également être `index.html` et non `Index.html`.

3. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

4. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.

5. Dans la liste des buckets, choisissez le nom du bucket que vous souhaitez utiliser pour héberger un site Web statique.

6. Activez l'hébergement de site Web statique pour votre compartiment et saisissez le nom exact de votre document d'index (par exemple, `index.html`). Pour plus d'informations, consultez Activation de l'hébergement de sites web.

   Après l'activation de l'hébergement de site web statique, passez à l'étape 6.

7. Pour charger le document d'index dans votre compartiment, effectuez l'une des opérations suivantes :

   - Faites glisser et déposez le fichier d'index dans la liste du compartiment de la console.
   - Choisissez Charger, puis suivez les instructions pour choisir et charger le fichier d'index.

   Pour step-by-step obtenir des instructions, voirChargement d'objets.

8. (Facultatif) Chargez du contenus d'un autre site Web dans votre compartiment.

Étape 6 : configurer un document d'erreur

Lorsque vous activez l'hébergement de site Web statique pour votre compartiment, vous entrez le nom du document d'erreur (par exemple, **`404.html`**). Après avoir activé l'hébergement de site web statique pour le compartiment, vous chargez un fichier HTML avec le nom du document d'erreur dans votre compartiment.

Pour configurer un document d'erreur

1. Créez un document d'erreur, par exemple `404.html`.
2. Enregistrez le fichier de document d'erreur au niveau local.

   Le nom du document d'erreur est sensible à la casse et doit correspondre exactement au nom que vous saisissez lorsque vous activez l'hébergement de site web statique. Par exemple, si vous entrez `404.html` pour le nom du document d'Erreur dans la boîte de dialogue Hébergement de site Web statique, le nom de fichier de votre document d'erreur doit également être `404.html`.
3. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
4. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
5. Dans la liste des buckets, choisissez le nom du bucket que vous souhaitez utiliser pour héberger un site Web statique.
6. Activez l'hébergement de site Web statique pour votre compartiment et entrez le nom exact de votre document d'erreur (par exemple, `404.html`). Pour plus d'informations, consultez Activation de l'hébergement de sites web et Configuration d'un document d'erreur personnalisé.

   Après l'activation de l'hébergement de site web statique, passez à l'étape 6.
7. Pour charger le document d'erreur dans votre compartiment, effectuez l'une des opérations suivantes :

   - Faites glisser et déposez le fichier du document d'erreur dans la liste des compartiments de la console.
   - Choisissez Upload (Charger), puis suivez les instructions pour choisir et charger le fichier d'index.

   Pour step-by-step obtenir des instructions, voirChargement d'objets.

Étape 7 : tester le point de terminaison de votre site web

Après avoir configuré l'hébergement de site web statique pour votre compartiment, vous pouvez tester le point de terminaison de votre site Web.

> **Note**
>
> Amazon S3 ne prend pas en charge l'accès HTTPS au site web. Si vous souhaitez utiliser le protocole HTTPS, vous pouvez utiliser Amazon CloudFront pour diffuser un site Web statique hébergé sur Amazon S3.
> Pour plus d'informations, consultez Comment utiliser CloudFront pour diffuser un site Web statique hébergé sur Amazon S3 ? et Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.

1. Dans Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Propriétés.
3. Au bas de la page, sous Héberger un site Web statique, choisissez le Point de terminaison du site Web du compartiment.

   Le document d'index s'ouvre dans une autre fenêtre du navigateur.

Vous avez désormais un site web hébergé sur Amazon S3. Ce site web est accessible au niveau du point de terminaison du site web Amazon S3. Néanmoins, vous devez avoir un domaine, de type `example.com`, pour proposer le contenu à partir du site web que vous avez créé. Vous pouvez également vouloir utiliser le domaine racine Amazon S3 pour traiter les demandes concernant `http://www.example.com` et `http://example.com`. Cela nécessite des étapes supplémentaires. Pour obtenir un exemple, consultez Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53.

Étape 8 : nettoyer

Si vous avez créé votre site web statique comme un simple exercice d'apprentissage, supprimez les ressources AWS que vous avez allouées afin de ne plus accumuler de frais. Une fois que vous avez supprimé vos AWS ressources, votre site Web n'est plus disponible. Pour de plus amples informations, veuillez consulter Supprimer un bucket à usage général.

Tutoriel : configuration d'un site Web statique à l'aide d'un domaine personnalisé enregistré auprès de Route 53

Admettons que vous souhaitiez héberger un site web statique sur Amazon S3. Vous avez enregistré un domaine auprès d'Amazon Route 53 (par exemple, `example.com`) et vous souhaitez que les

demandes concernant `http://www.example.com` et `http://example.com` soient servies à partir de votre contenu Amazon S3. Vous pouvez utiliser cette démonstration pour apprendre à héberger un site web statique et créer des redirections sur Amazon S3 pour un site web avec un nom de domaine personnalisé enregistré auprès de Route 53. Vous pouvez utiliser un site web existant que vous souhaitez héberger sur Amazon S3 ou utiliser cette démonstration pour commencer à partir de zéro.

Une fois cette procédure pas à pas terminée, vous pouvez éventuellement utiliser Amazon CloudFront pour améliorer les performances de votre site Web. Pour de plus amples informations, veuillez consulter Accélérez votre site Web avec Amazon CloudFront.

> **Note**
>
> Les points de terminaison de site web Amazon S3 ne prennent pas en charge le protocole HTTPS ou les points d'accès. Si vous souhaitez utiliser le protocole HTTPS, vous pouvez utiliser Amazon CloudFront pour diffuser un site Web statique hébergé sur Amazon S3. Pour un didacticiel expliquant comment héberger votre contenu en toute sécurité avec CloudFront Amazon S3, consultezTutoriel : Hébergement de vidéos en streaming à la demande avec Amazon S3 CloudFront, Amazon et Amazon Route 53. Pour plus d'informations, consultez Comment utiliser CloudFront pour diffuser un site Web statique hébergé sur Amazon S3 ? et Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.

Automatiser la configuration d'un site Web statique à l'aide d'un modèle AWS CloudFormation

Vous pouvez utiliser un AWS CloudFormation modèle pour automatiser la configuration statique de votre site Web. Le AWS CloudFormation modèle définit les composants dont vous avez besoin pour héberger un site Web statique sécurisé afin que vous puissiez vous concentrer davantage sur le contenu de votre site Web et moins sur la configuration des composants.

Le AWS CloudFormation modèle inclut les composants suivants :

- Amazon S3 – Crée un compartiment Amazon S3 pour héberger votre site web statique.
- CloudFront — Crée une CloudFront distribution pour accélérer votre site Web statique.
- Lambda@Edge – Utilise Lambda@Edge pour ajouter des en-têtes de sécurité à chaque réponse du serveur. Les en-têtes de sécurité sont un groupe d'en-têtes dans la réponse du serveur Web qui indiquent aux navigateurs web d'appliquer des mesures de sécurité supplémentaires. Pour plus

d'informations, consultez le billet de blog Ajouter des en-têtes de sécurité HTTP à l'aide de Lambda @Edge et Amazon. CloudFront

Ce AWS CloudFormation modèle est disponible pour que vous puissiez le télécharger et l'utiliser. Pour obtenir des informations et des instructions, consultez Getting started with a secure static website in the Amazon CloudFront Developer Guide.

Rubriques

- Avant de commencer
- Étape 1 : enregistrer un domaine personnalisé avec Route 53
- Étape 2 : créer deux compartiments
- Étape 3 : configurer votre compartiment de domaine racine pour l'hébergement de site web
- Étape 4 : configurer votre compartiment de sous-domaine pour la redirection de site web
- Étape 5 : configurer la journalisation pour le trafic du site web
- Étape 6 : charger l'index et le contenu du site web
- Étape 7 : charger un document d'erreur
- Étape 8 : modifier les paramètres de blocage de l'accès public S3
- Étape 9 : attacher une politique de compartiment
- Étape 10 : tester le point de terminaison de domaine
- Étape 11 : ajouter des enregistrements d'alias pour vos domaine et sous-domaine
- Étape 12 : tester le site web
- Accélérez votre site Web avec Amazon CloudFront
- Nettoyage de vos exemples de ressources

Avant de commencer

À mesure que vous suivez les étapes de cet exemple, vous utilisez les services suivants :

Amazon Route 53 – Vous utilisez Route 53 pour enregistrer des domaines et définir où vous souhaitez acheminer le trafic Internet pour votre domaine. Cet exemple montre comment créer des enregistrements d'alias Route 53 qui acheminent le trafic de votre domaine (`example.com`) et de votre sous-domaine (`www.example.com`) vers un compartiment Amazon S3 qui contient un fichier HTML.

Amazon S3 – Vous utilisez Amazon S3 pour créer des compartiments, charger un modèle de page de site web, configurer des autorisations afin que toute personne puisse consulter le contenu et ensuite configurer les compartiments pour l'hébergement de sites web.

Étape 1 : enregistrer un domaine personnalisé avec Route 53

Si vous ne disposez pas déjà d'un nom de domaine enregistré, tel que `example.com`, enregistrez-en un avec Route 53. Pour plus d'informations, consultez Enregistrement d'un nouveau domaine dans le Guide du développeur Amazon Route 53. Après avoir enregistré votre nom de domaine, vous pouvez créer et configurer vos compartiments Amazon S3 pour l'hébergement de sites web.

Étape 2 : créer deux compartiments

Pour prendre en charge les demandes à partir du domaine racine et du sous-domaine, vous créez deux compartiments.

- Compartiment de domaine – `example.com`
- Compartiment de sous-domaine – `www.example.com`

Ces noms de compartiment doivent correspondre exactement à votre nom de domaine. Dans cet exemple, le nom de domaine est `example.com`. Vous hébergez votre contenu hors du compartiment de domaine racine (`example.com`). Vous créez une demande de redirection pour le compartiment de sous-domaine (`www.example.com`). Si quelqu'un saisit `www.example.com` dans son navigateur, il est redirigé vers `example.com` et voit le contenu hébergé dans le compartiment Amazon S3 portant ce nom.

Pour créer des compartiments pour l'hébergement de site web

Les instructions ci-dessous fournissent une vue d'ensemble de la façon de créer vos compartiments pour l'hébergement de site web. Pour obtenir des step-by-step instructions détaillées sur la création d'un bucket, consultezCréation d'un bucket à usage général.

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Créez votre compartiment de domaine racine.

    a. Dans la barre de navigation en haut de la page, choisissez le nom du fichier actuellement affiché Région AWS. Choisissez ensuite la région dans laquelle vous souhaitez créer un compartiment.

> **Note**
>
> Pour limiter la latence et les coûts, et répondre aux exigences légales, choisissez une région proche de vous. Les objets stockés dans une Région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre Région. Pour obtenir la liste d'Amazon S3 Régions AWS, consultez la section sur les Service AWS points de terminaison dans le Référence générale d'Amazon Web Services.

b. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.

c. Choisissez Créer un compartiment. La page Créer un compartiment s'ouvre.

d. Saisissez le Nom du compartiment (par exemple **`example.com`**).

e. Choisissez la Région dans laquelle vous souhaitez créer le compartiment.

   Choisissez une Région proche de vous sur le plan géographique afin de limiter la latence et les coûts, ou de répondre aux exigences réglementaires. C'est la Région que vous choisissez qui détermine votre point de terminaison de site web Amazon S3. Pour plus d'informations, consultez Points de terminaison de sites web.

f. Pour accepter les paramètres par défaut et créer le compartiment, choisissez Créer.

3. Créez votre compartiment de sous-domaine :

   a. Choisissez Créer un compartiment.

   b. Saisissez le Nom du compartiment (par exemple **`www.example.com`**).

   c. Choisissez la Région dans laquelle vous souhaitez créer le compartiment.

      Choisissez une Région proche de vous sur le plan géographique afin de limiter la latence et les coûts, ou de répondre aux exigences réglementaires. C'est la Région que vous choisissez qui détermine votre point de terminaison de site web Amazon S3. Pour plus d'informations, consultez Points de terminaison de sites web.

   d. Pour accepter les paramètres par défaut et créer le compartiment, choisissez Créer.

Dans l'étape suivante, vous configurez `example.com` pour l'hébergement de site web.

Étape 3 : configurer votre compartiment de domaine racine pour l'hébergement de site web

Dans cette étape, vous configurez votre compartiment de domaine racine (`example.com`) en tant que site web. Ce compartiment contient le contenu de votre site web. Lorsque vous configurez un compartiment pour héberger un site web, vous pouvez accéder à ce site à l'aide des Points de terminaison de sites web.

Pour activer l'hébergement de site Web statique

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
3. Dans la liste des compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer l'hébergement statique de sites Web.
4. Choisissez Propriétés.
5. Sous Static website hosting (Hébergement de site Web statique), choisissez Edit (Modifier).
6. Choisissez Utiliser ce compartiment pour héberger un site Web.
7. Sous Static website hosting (Hébergement de site web statique), choisissez Enable (Activer).
8. Dans Index document (Document d'index), entrez le nom du document d'index, généralement `index.html`.

   Le nom du document d'index est sensible à la casse et doit correspondre exactement au nom de fichier du document d'index HTML que vous prévoyez de charger dans votre compartiment S3. Lorsque vous configurez un compartiment pour l'hébergement d'un site web, vous devez indiquer un document d'index. Amazon S3 renvoie ce document d'index lorsque des demandes sont faites dans le domaine racine ou dans n'importe quel sous-dossier. Pour plus d'informations, consultez Configuration d'un document d'index.
9. Pour fournir votre propre document d'erreur personnalisé pour les erreurs de classe 4XX, entrez le nom du fichier du document d'erreur personnalisé dans Document d'erreur.

   Le nom du document d'erreur est sensible à la casse et doit correspondre exactement au nom de fichier du document d'erreur HTML que vous prévoyez de charger dans votre compartiment S3. Si vous ne spécifiez pas de document d'erreur personnalisé et qu'une erreur se produit, Amazon S3 renvoie un document d'erreur HTML par défaut. Pour plus d'informations, consultez Configuration d'un document d'erreur personnalisé.

10. (Facultatif) Si vous souhaitez spécifier des règles de redirection avancées, décrivez les règles à l'aide du langage JSON dans Redirection rules (Règles de redirection).

    Par exemple, vous pouvez acheminer les demandes de façon conditionnelle en fonction des noms ou préfixes de clés d'objets dans la demande. Pour plus d'informations, consultez Configurer des règles de redirection pour utiliser des redirections conditionnelles avancées.
11. Choisissez Enregistrer les modifications.

    Amazon S3 permet l'hébergement de site web statique pour votre compartiment. Au bas de la page, sous Static website hosting (Hébergement de site Web statique), vous voyez le point de terminaison du site web pour votre compartiment.
12. Sous Static website hosting (Hébergement de site Web statique), notez la valeur de Endpoint (Point de terminaison).

    Endpoint (Point de terminaison) correspond au point de terminaison du site web Amazon S3 de votre compartiment. Une fois que vous avez terminé de configurer votre compartiment en tant que site Web statique, vous pouvez utiliser ce point de terminaison pour tester votre site Web.

Après avoir modifié les paramètres de blocage de l'accès public et ajouté une politique de compartiment qui autorise l'accès en lecture publique, vous pouvez utiliser le point de terminaison du site web pour accéder à votre site web.

Au cours de l'étape suivante, vous configurez votre sous-domaine (`www.example.com`) pour rediriger les demandes vers votre domaine (`example.com`).

Étape 4 : configurer votre compartiment de sous-domaine pour la redirection de site web

Maintenant que vous avez configuré le compartiment de votre domaine racine pour l'hébergement de site Web, vous pouvez configurer le compartiment de votre sous-domaine pour rediriger toutes les demandes vers le domaine. Dans cet exemple, toutes les demandes pour `www.example.com` sont redirigées vers `example.com`.

Pour configurer une demande de redirection

1. Sur la console Amazon S3, dans la liste des compartiments à usage général, choisissez le nom de votre compartiment de sous-domaine (`www.example.com`dans cet exemple).
2. Choisissez Propriétés.

3. Sous Static website hosting (Hébergement de site web statique), choisissez Edit (Modifier).
4. Choisissez Redirect requests for an object (Rediriger les demandes pour un objet).
5. Dans la zone Target bucket (Compartiment cible), entrez votre domaine racine, par exemple, **`example.com`**.
6. Pour Protocol (Protocole), choisissez http.
7. Choisissez Enregistrer les modifications.

Étape 5 : configurer la journalisation pour le trafic du site web

Si vous souhaitez effectuer le suivi du nombre de visiteurs accédant à votre site web, vous pouvez activer la journalisation pour le compartiment de votre domaine racine. Pour de plus amples informations, veuillez consulter Enregistrement de demandes avec journalisation des accès au serveur. Si vous envisagez d'utiliser Amazon CloudFront pour accélérer votre site Web, vous pouvez également utiliser la CloudFront journalisation.

Pour activer la journalisation des accès au serveur pour votre compartiment de domaine racine

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Dans la Région où vous avez créé le compartiment configuré en tant que site Web statique, créez un compartiment pour la journalisation, par exemple `logs.example.com`.
3. Créez un dossier pour les fichiers de journalisation des accès au serveur (par exemple, `logs`).
4. (Facultatif) Si vous souhaitez l'utiliser CloudFront pour améliorer les performances de votre site Web, créez un dossier pour les fichiers CloudFront journaux (par exemple,`cdn`).

> **Important**
>
> Lorsque vous créez ou mettez à jour une distribution et que vous activez la CloudFront journalisation, la liste de contrôle d'accès au compartiment (ACL) est mise à CloudFront jour pour autoriser le `awslogsdelivery` compte `FULL_CONTROL` à écrire des journaux dans votre compartiment. Pour plus d'informations, consultez la section Autorisations requises pour configurer la journalisation standard et pour accéder à vos fichiers journaux dans le manuel Amazon CloudFront Developer Guide. Si le compartiment qui stocke les journaux utilise le paramètre imposé par le propriétaire du compartiment pour désactiver la propriété des objets S3 ACLs, il CloudFront ne peut pas écrire de journaux

dans le compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

5. Dans la liste Compartiments choisissez votre compartiment de domaine racine.
6. Choisissez Propriétés.
7. Sous Server access logging (Journalisation des accès au serveur), choisissez Edit (Modifier).
8. Sélectionnez Activer.
9. Sous Target bucket (Compartiment cible), choisissez la destination du compartiment et du dossier pour les journaux d'accès au serveur :

   - Accédez à l'emplacement du dossier et du compartiment :
     1. Choisissez Parcourir S3.
     2. Choisissez le nom du compartiment, puis le dossier des journaux.
     3. Choisissez Choose path (Sélectionnez un chemin).
   - Saisissez le chemin du compartiment S3, par ex., `s3://logs.example.com/logs/`.
10. Choisissez Enregistrer les modifications.

    Dans votre compartiment de journaux, vous pouvez désormais accéder à vos journaux. Amazon S3 copie les journaux d'accès du site web dans votre compartiment de journaux toutes les deux heures.

Étape 6 : charger l'index et le contenu du site web

Dans cette étape, vous chargez votre document d'index et le contenu de site web facultatif dans votre compartiment de domaine racine.

Lorsque vous activez l'hébergement de site web statique pour votre compartiment, vous saisissez le nom du document d'index (par exemple, **`index.html`**). Après avoir activé l'hébergement de site web statique pour le compartiment, vous téléchargez un fichier HTML avec le nom du document de cet index dans votre compartiment.

Pour configurer le document d'index

1. Créez un fichier `index.html`.

   Si vous n'avez pas de ficher `index.html`, vous pouvez utiliser le code HTML suivant pour en créer un :

```
<html xmlns="http://www.w3.org/1999/xhtml" >
<head>
    <title>My Website Home Page</title>
</head>
<body>
  <h1>Welcome to my website</h1>
  <p>Now hosted on Amazon S3!</p>
</body>
</html>
```

2. Enregistrez le fichier d'index au niveau local.

   Le nom du fichier du document d'index doit correspondre exactement au nom du document d'index que vous saisissez dans la boîte de dialogue Hébergement de site Web statique. Le nom du document d'index est sensible à la casse. Par exemple, si vous saisissez `index.html` pour le nom du Document d'index dans la boîte de dialogue Hébergement de site Web statique, le nom du fichier de votre document d'index doit également être `index.html` et non `Index.html`.

3. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.

4. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.

5. Dans la liste des compartiments, choisissez le nom du compartiment que vous souhaitez utiliser pour héberger un site Web statique.

6. Activez l'hébergement de site Web statique pour votre compartiment et saisissez le nom exact de votre document d'index (par exemple, `index.html`). Pour plus d'informations, consultez Activation de l'hébergement de sites web.

   Après l'activation de l'hébergement de site web statique, passez à l'étape 6.

7. Pour charger le document d'index dans votre compartiment, effectuez l'une des opérations suivantes :

   - Faites glisser et déposez le fichier d'index dans la liste du compartiment de la console.
   - Choisissez Charger, puis suivez les instructions pour choisir et charger le fichier d'index.

   Pour step-by-step obtenir des instructions, voirChargement d'objets.

8. (Facultatif) Chargez du contenus d'un autre site Web dans votre compartiment.

Étape 7 : charger un document d'erreur

Lorsque vous activez l'hébergement de site Web statique pour votre compartiment, vous entrez le nom du document d'erreur (par exemple, **`404.html`**). Après avoir activé l'hébergement de site web statique pour le compartiment, vous chargez un fichier HTML avec le nom du document d'erreur dans votre compartiment.

Pour configurer un document d'erreur

1. Créez un document d'erreur, par exemple `404.html`.
2. Enregistrez le fichier de document d'erreur au niveau local.

   Le nom du document d'erreur est sensible à la casse et doit correspondre exactement au nom que vous saisissez lorsque vous activez l'hébergement de site web statique. Par exemple, si vous entrez `404.html` pour le nom du document d'Erreur dans la boîte de dialogue Hébergement de site Web statique, le nom de fichier de votre document d'erreur doit également être `404.html`.
3. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
4. Dans le volet de navigation de gauche, choisissez Compartiments à usage général.
5. Dans la liste des compartiments, choisissez le nom du compartiment que vous souhaitez utiliser pour héberger un site Web statique.
6. Activez l'hébergement de site Web statique pour votre compartiment et entrez le nom exact de votre document d'erreur (par exemple, `404.html`). Pour plus d'informations, consultez Activation de l'hébergement de sites web et Configuration d'un document d'erreur personnalisé.

   Après l'activation de l'hébergement de site web statique, passez à l'étape 6.
7. Pour charger le document d'erreur dans votre compartiment, effectuez l'une des opérations suivantes :

   - Faites glisser et déposez le fichier du document d'erreur dans la liste des compartiments de la console.
   - Choisissez Upload (Charger), puis suivez les instructions pour choisir et charger le fichier d'index.

   Pour step-by-step obtenir des instructions, voirChargement d'objets.

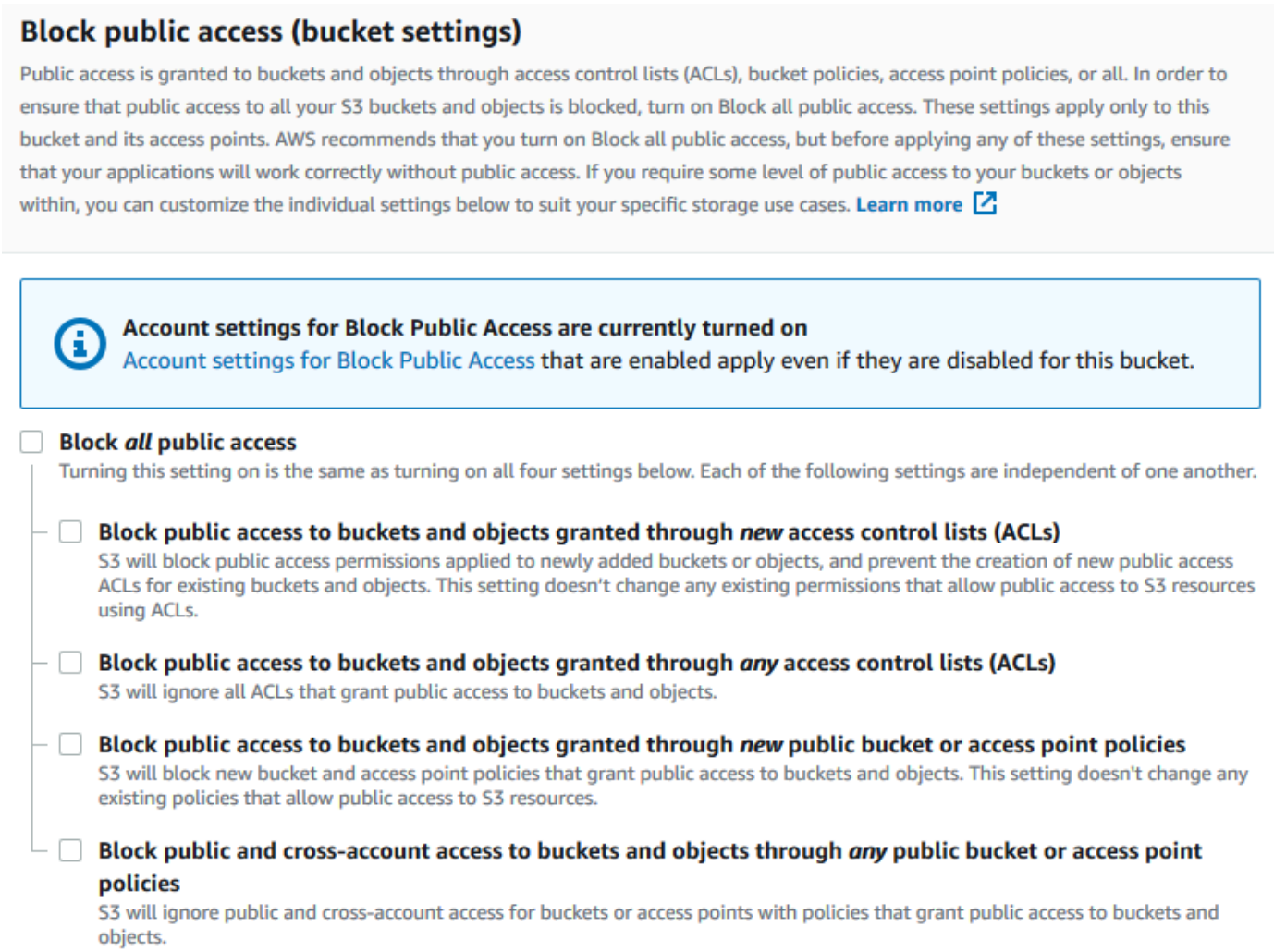
Étape 8 : modifier les paramètres de blocage de l'accès public S3

Dans cet exemple, vous modifiez les paramètres de blocage de l'accès public pour le compartiment de domaine (`example.com`) pour autoriser l'accès public.

Par défaut, Amazon S3 bloque l'accès public à votre compte et à vos compartiments. Si vous souhaitez utiliser un compartiment pour héberger un site web statique, vous pouvez utiliser ces étapes pour modifier vos paramètres de blocage de l'accès public.

> **Warning**
>
> Avant de suivre ces étapes, passez en revue Blocage de l'accès public à votre stockage Amazon S3 pour vous assurer que vous comprenez et acceptez les risques liés à l'autorisation de l'accès public. Lorsque vous désactivez les paramètres de blocage de l'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tous les accès publics à vos compartiments.

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le nom du compartiment que vous avez configuré en tant que site web statique.
3. Choisissez Permissions.
4. Sous Block public access (bucket settings) (Bloquer l'accès public (paramètres de compartiment)), choisissez Edit (Modifier).
5. Décochez Bloquer tous les accès publics et sélectionnez Enregistrer les modifications.



Amazon S3 désactive les paramètres de blocage de l'accès public pour votre compartiment. Pour créer un site Web public statique, vous devrez peut-être aussi modifier les paramètres de blocage de l'accès public de votre compte avant d'ajouter une politique de compartiment. Si les paramètres de blocage de l'accès public pour votre compte sont actuellement activés, une note s'affiche sous Bloquer l'accès public (paramètres de compartiment).

Étape 9 : attacher une politique de compartiment

Dans cet exemple, vous attachez une politique de compartiment au compartiment de domaine (`example.com`) pour autoriser l'accès public en lecture. Vous remplacez la politique de compartiment indiquée *`Bucket-Name`* dans l'exemple par le nom de votre compartiment de domaine, par exemple`example.com`.

Après avoir modifié les paramètres de blocage de l'accès public S3, vous devez ajouter une politique de compartiment pour accorder un accès public en lecture à votre compartiment. Lorsque vous accordez un accès public en lecture, tout le monde sur Internet peut accéder à votre compartiment.

> **Important**
>
> La stratégie suivante est uniquement un exemple et autorise un accès complet au contenu de votre compartiment. Avant d'effectuer cette étape, consultez Comment assurer la sécurité des fichiers de mon compartiment Amazon S3 ?, pour vous assurer que vous comprenez les bonnes pratiques pour sécuriser les fichiers dans votre compartiment S3 et les risques liés à l'octroi d'un accès public.

1. Dans Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Permissions.
3. Sous Politique de compartiment, choisissez Modifier.
4. Pour accorder l'accès public en lecture à votre site web, copiez la politique de compartiment suivante et collez-la dans l'Éditeur de politique de compartiment.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PublicReadGetObject",
            "Effect": "Allow",
            "Principal": "*",
            "Action": [
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::Bucket-Name/*"
            ]
        }
    ]
}
```

5. Mettez à jour `Resource` pour inclure le nom de votre compartiment.

   Dans l'exemple de politique de compartiment précédent, *`Bucket-Name`* il s'agit d'un espace réservé pour le nom du compartiment. Pour utiliser cette politique de compartiment avec votre

propre compartiment, vous devez mettre à jour ce nom pour qu'il corresponde à celui de votre compartiment.

6. Sélectionnez Enregistrer les modifications.

   Un message s'affiche indiquant que la politique de compartiment a été ajoutée avec succès.

   Si une erreur indique `Policy has invalid resource`, confirmez que le nom du compartiment dans la politique de compartiment correspond au nom de votre compartiment. Pour plus d'informations sur l'ajout d'une politique de compartiment, consultez Comment ajouter une politique de compartiment S3 ?

   Si vous recevez un message d'erreur et que vous ne pouvez pas enregistrer la stratégie de compartiment, vérifiez les paramètres de blocage de l'accès public de votre compte et de votre compartiment pour confirmer que vous autorisez l'accès public au compartiment.

Au cours de l'étape suivante, vous pouvez déterminer vos points de terminaison de site web et tester le point de terminaison de votre domaine.

Étape 10 : tester le point de terminaison de domaine

Après avoir configuré votre compartiment de domaine pour héberger un site web public, vous pouvez tester votre point de terminaison. Pour plus d'informations, consultez Points de terminaison de sites web. Vous pourrez uniquement tester le point de terminaison pour votre compartiment de domaine puisque votre compartiment de sous-domaine est configuré pour rediriger le site web et non pour l'hébergement de site web statique.

> **Note**
>
> Amazon S3 ne prend pas en charge l'accès HTTPS au site web. Si vous souhaitez utiliser le protocole HTTPS, vous pouvez utiliser Amazon CloudFront pour diffuser un site Web statique hébergé sur Amazon S3.
> Pour plus d'informations, consultez Comment utiliser CloudFront pour diffuser un site Web statique hébergé sur Amazon S3 ? et Exiger le protocole HTTPS pour la communication entre les spectateurs et CloudFront.

1. Dans Compartiments, choisissez le nom de votre compartiment.
2. Choisissez Propriétés.

3. Au bas de la page, sous Héberger un site Web statique, choisissez le Point de terminaison du site Web du compartiment.

   Le document d'index s'ouvre dans une autre fenêtre du navigateur.

À l'étape suivante, vous utiliserez Amazon Route 53 pour permettre aux clients d'utiliser vos deux options personnalisées URLs pour accéder à votre site.

Étape 11 : ajouter des enregistrements d'alias pour vos domaine et sous-domaine

Dans cette étape, vous créez les enregistrements d'alias que vous ajoutez à la zone hébergée pour que le domaine mappe `example.com` et `www.example.com`. Au lieu d'utiliser des adresses IP, les enregistrements d'alias utilisent les points de terminaison du site Web Amazon S3. Amazon Route 53 conserve un mappage entre les enregistrements d'alias et les adresses IP où résident les compartiments Amazon S3. Vous créez deux enregistrements d'alias, l'un pour votre domaine racine et l'autre pour votre sous-domaine.

Ajouter un enregistrement d'alias pour votre domaine racine et votre sous-domaine

Pour ajouter un enregistrement d'alias pour votre domaine racine (**`example.com`**)

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.

   > **Note**
   >
   > Si vous n'utilisez pas déjà Route 53, consultez Étape 1 : enregistrer un domaine dans le guide du développeur Amazon Route 53. Une fois la configuration terminée, vous pouvez reprendre les instructions.

2. Choisissez Hosted Zones (Zones hébergées).
3. Dans la liste des zones hébergées, choisissez le nom de la zone hébergée qui correspond au nom de votre domaine.
4. Choisissez Create Record (Créer un enregistrement).
5. Choisissez Switch to wizard (Passer à l'assistant).

> **Note**
>
> Si vous souhaitez utiliser la création rapide pour créer vos enregistrements d'alias, consultez Configuration de Route 53 pour acheminer le trafic vers un compartiment S3.

6. Choisissez Simple routing (Routage simple), puis Next (Suivant).
7. Choisissez Définir un enregistrement simple.
8. Dans Record name (Nom de registre), acceptez la valeur par défaut, à savoir le nom de votre zone hébergée et de votre domaine.
9. Dans Value/Route traffic to (Valeur/Acheminer le trafic vers), choisissez Alias to S3 website endpoint (Alias vers le point de terminaison du site web S3).
10. Choisissez la Région.
11. Choisissez le compartiment S3.

    Le nom du compartiment doit correspondre au nom qui apparaît dans la zone Nom. Dans la liste Choose S3 bucket (Choisir un compartiment S3), le nom du compartiment apparaît avec le point de terminaison de site Web Amazon S3 pour la Région où le compartiment a été créé, par exemple `s3-website-us-west-1.amazonaws.com (example.com)`.

    Choose S3 bucket (Choisir un compartiment S3) répertorie un compartiment si :

    - Vous avez configuré le compartiment en tant que site web statique.
    - Le nom du compartiment est identique au nom de l'enregistrement que vous créez.
    - Le courant Compte AWS a créé le compartiment.

    Si votre compartiment n'apparaît pas dans la liste Choose S3 bucket (Choisir un compartiment S3), saisissez le point de terminaison de site Web Amazon S3 de la Région dans laquelle le compartiment a été créé, par exemple, **`s3-website-us-west-2.amazonaws.com`**. Pour obtenir la liste complète des points de terminaison de sites Web Amazon S3, consultez Points de terminaison de sites Web Amazon S3. Pour en savoir plus sur la cible d'alias, consultez Valeur/acheminer le trafic vers dans le guide du développeur Amazon Route 53.
12. Dans Type d'enregistrement, choisissez A - Route le trafic vers une IPv4 adresse et certaines AWS ressources.
13. Pour Évaluer l'état de la cible, choisissez Non.
14. Choisissez Définir un enregistrement simple.

Pour ajouter un enregistrement d'alias pour votre sous-domaine (**`www.example.com`**)

1. Sous Configurer les enregistrements, choisissez Définir un enregistrement simple.
2. Dans Record name (Nom de registre) pour votre sous-domaine, tapez `www`.
3. Dans Value/Route traffic to (Valeur/Acheminer le trafic vers), choisissez Alias to S3 website endpoint (Alias vers le point de terminaison du site web S3).
4. Choisissez la Région.
5. Choisissez le compartiment S3, par exemple, `s3-website-us-west-2.amazonaws.com (www.example.com)`.

   Si votre compartiment n'apparaît pas dans la liste Choose S3 bucket (Choisir un compartiment S3), saisissez le point de terminaison de site Web Amazon S3 de la Région dans laquelle le compartiment a été créé, par exemple, **`s3-website-us-west-2.amazonaws.com`**. Pour obtenir la liste complète des points de terminaison de sites Web Amazon S3, consultez Points de terminaison de sites Web Amazon S3. Pour en savoir plus sur la cible d'alias, consultez Valeur/acheminer le trafic vers dans le guide du développeur Amazon Route 53.
6. Dans Type d'enregistrement, choisissez A - Route le trafic vers une IPv4 adresse et certaines AWS ressources.
7. Pour Évaluer l'état de la cible, choisissez Non.
8. Choisissez Définir un enregistrement simple.
9. Dans la page Configurer des enregistrements, choisissez Créer des enregistrements.

> **Note**
>
> Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous pouvez acheminer le trafic vers votre compartiment Amazon S3 en utilisant les noms des enregistrements d'alias que vous avez créés au cours de cette procédure.

Ajouter un enregistrement d'alias pour votre domaine racine et votre sous-domaine (ancienne console Route 53)

Pour ajouter un enregistrement d'alias pour votre domaine racine (**`example.com`**)

La console Route 53 a été repensée. Dans la console Route 53, vous pouvez temporairement utiliser l'ancienne console. Si vous choisissez d'utiliser l'ancienne console Route 53, suivez la procédure ci-dessous.

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.

   > **Note**
   >
   > Si vous n'utilisez pas déjà Route 53, consultez Étape 1 : enregistrer un domaine dans le guide du développeur Amazon Route 53. Une fois la configuration terminée, vous pouvez reprendre les instructions.

2. Choisissez Hosted Zones (Zones hébergées).
3. Dans la liste des zones hébergées, choisissez le nom de la zone hébergée qui correspond au nom de votre domaine.
4. Choisissez Create Record Set (Créer un ensemble d'enregistrements).
5. Indiquez l'une des valeurs suivantes :

   Nom

   Acceptez la valeur par défaut, à savoir le nom de votre zone hébergée et de votre domaine.

   Pour le domaine racine, vous n'avez pas besoin d'entrer des informations supplémentaires dans le champ Nom.

   Type

   Choisissez A — IPv4 adresse.

   Alias

   Choisissez Yes (Oui).

   Cible d'alias

   Dans la section S3 website endpoints (Points de terminaison de site web S3) de la liste, choisissez le nom de votre compartiment.

Le nom du compartiment doit correspondre au nom qui apparaît dans la zone Nom. Dans la liste Alias Target (Cible d'alias), le nom du compartiment est suivi du point de terminaison du site web Amazon S3 pour la Région dans laquelle le compartiment a été créé, par exemple `example.com (s3-website-us-west-2.amazonaws.com)`. Alias Target (Cible d'alias) répertorie un compartiment si :

- Vous avez configuré le compartiment en tant que site web statique.
- Le nom du compartiment est identique au nom de l'enregistrement que vous créez.
- Le courant Compte AWS a créé le compartiment.

Si votre compartiment n'apparaît pas dans la liste Alias Target (Cible d'alias), saisissez le point de terminaison du site web Amazon S3 pour la Région dans laquelle le compartiment a été créé, par exemple, `s3-website-us-west-2`. Pour obtenir la liste complète des points de terminaison de sites Web Amazon S3, consultez Points de terminaison de sites Web Amazon S3. Pour en savoir plus sur la cible d'alias, consultez Valeur/acheminer le trafic vers dans le guide du développeur Amazon Route 53.

Stratégie de routage

Acceptez la valeur par défaut Simple.

Évaluer l'état de la cible

Acceptez la valeur par défaut Non.

6. Choisissez Créer.

Pour ajouter un enregistrement d'alias pour votre sous-domaine (**`www.example.com`**)

1. Dans la zone hébergée pour votre domaine racine (`example.com`), choisissez Create Record Set (Créer un jeu d'enregistrements).
2. Indiquez l'une des valeurs suivantes :

   Nom

   Pour le sous-domaine, entrez `www` dans la zone.

   Type

   Choisissez A — IPv4 adresse.

Alias

Choisissez Yes (Oui).

Cible d'alias

Dans la section Points de terminaison de site web S3 de la liste, choisissez le même nom de compartiment que celui qui apparaît dans le champ Nom, par exemple `www.example.com (s3-website-us-west-2.amazonaws.com)`.

Stratégie de routage

Acceptez la valeur par défaut Simple.

Évaluer l'état de la cible

Acceptez la valeur par défaut Non.

3. Choisissez Créer.

> **Note**
>
> Les changements se propagent généralement sur tous les serveurs Route 53 en 60 secondes. Lorsque la propagation est terminée, vous pouvez acheminer le trafic vers votre compartiment Amazon S3 en utilisant les noms des enregistrements d'alias que vous avez créés au cours de cette procédure.

Étape 12 : tester le site web

Vérifiez que le site web et la redirection fonctionnent correctement. Dans votre navigateur, saisissez votre URLs. Dans cet exemple, vous pouvez essayer ce qui suit URLs :

- Domaine (`http://example.com`) – Affiche le document d'index dans le compartiment `example.com`.
- Sous-domaine (`http://www.example.com`) – Redirige votre demande vers `http://example.com`. Vous voyez le document d'index dans le compartiment `example.com`.

Si votre site web ou les liens de redirection ne fonctionnent pas, vous pouvez essayer la procédure suivante :

- Effacer le cache – Effacez le cache de votre navigateur web.
- Vérifier les serveurs de noms – Si votre page web et les liens de redirection ne fonctionnent pas une fois que vous avez effacé votre cache, vous pouvez comparer les serveurs de noms de votre domaine et les serveurs de noms de votre zone hébergée. Si les serveurs de noms ne correspondent pas, vous devrez peut-être mettre à jour vos serveurs de noms de domaine pour qu'ils correspondent à ceux répertoriés dans votre zone hébergée. Pour plus d'informations, consultez Ajout ou modification de serveurs de noms et d'enregistrements de type glue pour un domaine.

Après avoir testé avec succès votre domaine racine et votre sous-domaine, vous pouvez configurer une CloudFront distribution Amazon pour améliorer les performances de votre site Web et fournir des journaux que vous pouvez utiliser pour examiner le trafic du site Web. Pour de plus amples informations, veuillez consulter Accélérez votre site Web avec Amazon CloudFront.

Accélérez votre site Web avec Amazon CloudFront

Vous pouvez utiliser Amazon CloudFront pour améliorer les performances de votre site Web Amazon S3. CloudFront met les fichiers de votre site Web (tels que le HTML, les images et les vidéos) à disposition depuis les centres de données du monde entier (appelés emplacements périphériques). Lorsqu'un visiteur demande un fichier à votre site web, CloudFront redirige automatiquement la demande vers une copie du fichier située à l'emplacement périphérique le plus proche. Le temps de téléchargement est alors plus rapide que si le visiteur avait demandé le contenu à un centre de données plus éloigné.

CloudFront met en cache le contenu aux emplacements périphériques pendant une période que vous spécifiez. Si un visiteur demande un contenu mis en cache depuis plus longtemps que la date d'expiration, CloudFront vérifie sur le serveur d'origine si une version plus récente du contenu est disponible. Si une version plus récente est disponible, CloudFront copie la nouvelle version vers l'emplacement périphérique. Les modifications que vous apportez au contenu d'origine sont répliquées aux emplacements périphériques lorsque les visiteurs demandent ce contenu.

Utilisation CloudFront sans Route 53

Le didacticiel de cette page utilise Route 53 pour pointer vers votre CloudFront distribution. Toutefois, si vous souhaitez diffuser du contenu hébergé dans un compartiment Amazon S3 CloudFront sans utiliser Route 53, consultez les CloudFrontdidacticiels Amazon : Configuration d'une distribution dynamique de contenu pour Amazon S3. Lorsque vous diffusez du contenu hébergé dans un

compartiment Amazon S3 à l'aide de CloudFront, vous pouvez utiliser n'importe quel nom de compartiment, et les protocoles HTTP et HTTPS sont pris en charge.

Automatiser la configuration à l'aide d'un modèle AWS CloudFormation

Pour plus d'informations sur l'utilisation d'un AWS CloudFormation modèle pour configurer un site Web statique sécurisé qui crée une CloudFront distribution destinée à votre site Web, consultez Getting started with a secure static website dans le manuel Amazon CloudFront Developer Guide.

Rubriques

- Étape 1 : Création d'une CloudFront distribution
- Étape 2 : Mettre à jour les jeux d'enregistrements pour votre domaine et votre sous-domaine
- (Facultatif) Étape 3 : Vérifier les fichiers journaux

Étape 1 : Création d'une CloudFront distribution

Tout d'abord, vous créez une CloudFront distribution. Votre site web est ainsi disponible à partir de centres de données dans le monde entier.

Pour créer une distribution avec une origine Amazon S3

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Choisissez Create Distribution.
3. Sur la page Créer une distribution dans la section Paramètres d'origine pour le Nom du domaine d'origine, saisissez le point de terminaison du site web Amazon S3 pour votre compartiment, par exemple, **`example.com.s3-website.us-west-1.amazonaws.com`**.

   CloudFront renseigne l'ID d'origine pour vous.
4. Pour Paramètres de comportement du cache par défaut, conservez les valeurs par défaut.

   Avec les paramètres par défaut de Stratégie de protocole d'utilisateur, vous pouvez utiliser HTTPS pour votre site web statique. Pour plus d'informations sur ces options de configuration, consultez la section Valeurs que vous spécifiez lorsque vous créez ou mettez à jour une distribution Web dans le manuel Amazon CloudFront Developer Guide.
5. Pour Paramètres de distribution, procédez comme suit :

   a. Laissez le paramètre Catégorie de tarifs défini sur Utiliser tous les emplacements périphériques (meilleure performance).

b. Définissez les noms de domaine alternatifs (CNAMEs) pour le domaine racine et le `www` sous-domaine. Dans le présent didacticiel, ce sont `example.com` et `www.example.com`.

> **Important**
>
> Avant d'effectuer cette étape, notez les exigences relatives à l'utilisation de noms de domaines alternatifs, en particulier la nécessité d'avoir un certificat SSL/TLS valide.

c. Pour Certificat SSL, choisissez Certificat SSL personnalisé (example.com), puis choisissez le certificat personnalisé qui couvre les noms de domaine et de sous-domaine.

   Pour plus d'informations, consultez la section Certificat SSL dans le manuel Amazon CloudFront Developer Guide.

d. Dans Objet racine par défaut, entrez le nom de votre document d'index, par exemple `index.html`.

   Si l'URL utilisée pour accéder à la distribution ne contient pas de nom de fichier, la CloudFront distribution renvoie le document d'index. L'objet racine par défaut doit correspondre exactement au nom du document d'index de votre site web statique. Pour plus d'informations, consultez Configuration d'un document d'index.

e. Définissez Journalisation sur Activé.

> **Important**
>
> Lorsque vous créez ou mettez à jour une distribution et que vous activez la CloudFront journalisation, la liste de contrôle d'accès au compartiment (ACL) est mise à CloudFront jour pour autoriser le `awslogsdelivery` compte `FULL_CONTROL` à écrire des journaux dans votre compartiment. Pour plus d'informations, consultez la section Autorisations requises pour configurer la journalisation standard et pour accéder à vos fichiers journaux dans le manuel Amazon CloudFront Developer Guide. Si le compartiment qui stocke les journaux utilise le paramètre imposé par le propriétaire du compartiment pour désactiver la propriété des objets S3 ACLs, il CloudFront ne peut pas écrire de journaux dans le compartiment. Pour de plus amples informations, veuillez consulter Contrôle de la propriété des objets et désactivation ACLs pour votre compartiment.

f. Pour Compartiment pour les journaux, choisissez le compartiment de journalisation que vous avez créé.

   Pour plus d'informations sur la configuration d'un compartiment de journalisation, consultez (Facultatif) Journalisation du trafic web.

g. Si vous souhaitez stocker les journaux générés par le trafic dans la distribution CloudFront dans un dossier, dans Préfixe de journal, entrez le nom du dossier.

h. Conservez tous les autres paramètres sur leurs valeurs par défaut.

6. Choisissez Create Distribution.

7. Pour voir le statut de la distribution, recherchez cette dernière dans la console et examinez la colonne Statut.

   Le statut `InProgress` indique que la distribution n'est pas encore pleinement déployée.

   Une fois que la distribution est déployée, vous pouvez référencer votre contenu avec le nouveau nom de domaine CloudFront.

8. Enregistrez la valeur du nom de domaine affiché dans la CloudFront console, par exemple`dj4p1rv6mvubz.cloudfront.net`.

9. Pour vérifier que votre CloudFront distribution fonctionne, entrez le nom de domaine de la distribution dans un navigateur Web.

   Si votre site Web est visible, la CloudFront distribution fonctionne. Si votre site Web possède un domaine personnalisé enregistré auprès d'Amazon Route 53, vous aurez besoin du nom de CloudFront domaine pour mettre à jour l'ensemble d'enregistrements à l'étape suivante.

Étape 2 : Mettre à jour les jeux d'enregistrements pour votre domaine et votre sous-domaine

Maintenant que vous avez créé une CloudFront distribution avec succès, mettez à jour l'enregistrement d'alias dans Route 53 pour qu'il pointe vers la nouvelle CloudFront distribution.

Pour mettre à jour l'enregistrement d'alias afin qu'il pointe vers une CloudFront distribution

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.

2. Dans le volet gauche de navigation, choisissez Hosted zones (Zones hébergées).

3. Sur la page Hosted Zones (Zones hébergées), choisissez la zone hébergée que vous avez créée pour votre sous-domaine, par exemple `www.example.com`.

4. Sous Records (Enregistrements), sélectionnez l'enregistrement A que vous avez créé pour votre sous-domaine.
5. Sous Record details (Détails de l'enregistrement), choisissez Edit record (Modifier l'enregistrement).
6. Sous Acheminer le trafic vers, choisissez Alias vers CloudFront la distribution.
7. Sous Choisir une distribution, choisissez la CloudFront distribution.
8. Choisissez Save (Enregistrer).
9. Pour rediriger l'enregistrement A du domaine racine vers la CloudFront distribution, répétez cette procédure pour le domaine racine, par exemple`example.com`.

   La mise à jour des jeux d'enregistrements prend effet dans un délai de 2 à 48 heures.
10. Pour voir si les nouveaux enregistrements A ont pris effet, entrez l'URL de votre sous-domaine dans un navigateur web, par exemple `http://www.example.com`.

    Si le navigateur ne vous redirige plus vers le domaine racine (par exemple `http://example.com`), les nouveaux enregistrements A sont en place. Lorsque le nouvel enregistrement A prend effet, le trafic acheminé par le nouvel enregistrement A vers la CloudFront distribution n'est pas redirigé vers le domaine racine. Tous les visiteurs qui font référence au site en utilisant `http://example.com` ou `http://www.example.com` sont redirigés vers l'emplacement CloudFront périphérique le plus proche, où ils bénéficient de temps de téléchargement plus rapides.

> **Tip**
>
> Les navigateurs peuvent mettre en cache les paramètres de redirection. Si vous pensez que les paramètres du nouvel enregistrement A devraient avoir pris effet mais que votre navigateur redirige encore `http://www.example.com` vers `http://example.com`, essayez d'effacer le cache et l'historique de votre navigateur, de fermer et de rouvrir votre application de navigateur, ou d'utiliser un navigateur web différent.

(Facultatif) Étape 3 : Vérifier les fichiers journaux

Les journaux d'accès vous indiquent combien de personnes visitent le site web. Ils contiennent également des données professionnelles utiles que vous pouvez analyser avec d'autres services, tels que Amazon EMR.

CloudFront les journaux sont stockés dans le compartiment et le dossier que vous choisissez lorsque vous créez une CloudFront distribution et que vous activez la journalisation. CloudFront écrit des journaux dans votre bucket de journaux dans les 24 heures suivant l'envoi des demandes correspondantes.

Pour consulter les fichiers journaux de votre site Web

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Choisissez le nom du compartiment de journaux pour votre site web.
3. Choisissez le dossier CloudFront des journaux.
4. Téléchargez les `.gzip` fichiers écrits par CloudFront avant de les ouvrir.

   Si vous avez créé votre site web comme un simple exercice d'apprentissage, vous pouvez supprimer les ressources que vous avez allouées afin de ne plus accumuler de frais. Pour ce faire, consultez Nettoyage de vos exemples de ressources. Une fois que vous avez supprimé vos ressources AWS , votre site web n'est plus disponible.

Nettoyage de vos exemples de ressources

Si vous avez créé votre site web statique dans le cadre d'un exercice d'apprentissage, veillez à supprimer les ressources AWS que vous avez allouées afin de ne plus accumuler de frais. Une fois que vous avez supprimé vos ressources AWS , votre site web n'est plus disponible.

Tâches

- Étape 1 : supprimer la CloudFront distribution Amazon
- Étape 2 : Supprimer la zone hébergée Route 53
- Étape 3 : Désactivez la journalisation et supprimez votre compartiment S3

Étape 1 : supprimer la CloudFront distribution Amazon

Avant de supprimer une CloudFront distribution Amazon, vous devez la désactiver. Une distribution désactivée n'est plus fonctionnelle et n'accumule pas de frais. Vous pouvez activer une distribution désactivée à tout moment. Une fois que vous avez supprimé une distribution désactivée, celle-ci n'est plus disponible.

Pour désactiver et supprimer une CloudFront distribution

1. Ouvrez la CloudFront console à l'adressehttps://console.aws.amazon.com/cloudfront/v4/home.
2. Sélectionnez la distribution que vous souhaitez désactiver, puis choisissez Désactiver).
3. Lorsque vous serez invité à confirmer l'opération, choisissez Oui, désactiver.
4. Sélectionnez la distribution désactivée, puis choisissez Supprimer.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Oui, supprimer.

Étape 2 : Supprimer la zone hébergée Route 53

Avant de supprimer la zone hébergée, vous devez supprimer les jeux d'enregistrements que vous avez créés. Vous n'avez pas besoin de supprimer les enregistrements NS et SOA ; ils sont automatiquement supprimés lorsque vous supprimez la zone hébergée.

Pour supprimer les jeux d'enregistrements

1. Ouvrez la console Route 53 à l'adresse https://console.aws.amazon.com/route53/.
2. Dans la liste des noms de domaines, sélectionnez votre nom de domaine, puis choisissez Go to Record Sets (Accéder aux jeux d'enregistrements).
3. Dans la liste des jeux d'enregistrement, sélectionnez les enregistrements A que vous avez créés.

   Le type de chaque jeu d'enregistrements est répertorié dans la colonne Type.
4. Choisissez Delete Record Set.
5. Lorsque vous êtes invité à confirmer l'opération, choisissez Confirm (Confirmer).

Pour supprimer une zone hébergée Route 53

1. Suite à la procédure précédente, choisissez Back to Hosted Zones (Retour aux zones hébergées).
2. Sélectionnez votre nom de domaine, puis choisissez Supprimer une zone hébergée.
3. Lorsque vous êtes invité à confirmer l'opération, choisissez Confirm (Confirmer).

Étape 3 : Désactivez la journalisation et supprimez votre compartiment S3

Avant de supprimer votre compartiment S3, assurez-vous que la journalisation est désactivée pour le compartiment. Sinon, AWS continue d'écrire des journaux dans votre compartiment lorsque vous le supprimez.

Pour désactiver la journalisation pour un compartiment

1. Ouvrez la console Amazon S3 à l'adresse https://console.aws.amazon.com/s3/.
2. Sous Compartiments, choisissez le nom de votre compartiment, puis choisissez Propriétés.
3. Dans Properties (Propriétés), choisissez Logging (Journalisation).
4. Désactivez la case à cocher Activé.
5. Choisissez Enregistrer.

Vous pouvez maintenant supprimer votre compartiment. Pour de plus amples informations, veuillez consulter Supprimer un bucket à usage général.

Déploiement d'un site Web statique vers AWS Amplify Hosting à partir d'un compartiment S3 à usage général

Nous vous recommandons d'utiliser AWS Amplify Hosting pour héberger le contenu d'un site Web statique stocké dans S3. Amplify Hosting est un service entièrement géré qui facilite le déploiement de vos sites Web sur un réseau de diffusion de contenu (CDN) disponible dans le monde entier alimenté par Amazon CloudFront, permettant un hébergement de sites Web statique sécurisé sans configuration approfondie. Avec AWS Amplify Hosting, vous pouvez sélectionner l'emplacement de vos objets dans votre compartiment à usage général, déployer votre contenu sur un CDN géré et générer une URL HTTPS publique pour que votre site Web soit accessible partout. Le déploiement d'un site Web statique à l'aide d'Amplify Hosting vous offre les avantages et fonctionnalités suivants :

- Le déploiement sur le réseau de diffusion de AWS contenu (CDN) géré par Amazon CloudFront CloudFront est un service Web qui accélère la distribution de votre contenu Web statique et dynamique à vos utilisateurs. CloudFront diffuse votre contenu par le biais d'un réseau mondial de centres de données appelés emplacements périphériques. Lorsqu'un utilisateur demande le contenu que vous diffusez CloudFront, la demande est acheminée vers l'emplacement périphérique offrant le moins de latence (délai), afin que le contenu soit diffusé avec les meilleures performances possibles, ainsi qu'une fiabilité et une disponibilité accrues. Pour plus d'informations,

consultez la section Comment CloudFront diffuse le contenu dans le manuel Amazon CloudFront Developer Guide.

- Prise en charge HTTPS : assure une communication et un transfert de données sécurisés entre votre site Web et le navigateur Web d'un utilisateur.
- Domaines personnalisés : connectez facilement votre site Web à une URL personnalisée achetée auprès d'un bureau d'enregistrement de domaines tel qu'Amazon Route 53.
- Certificats SSL personnalisés : lorsque vous configurez votre domaine personnalisé, vous pouvez utiliser le certificat géré par défaut que vous fournit Amplify ou vous pouvez utiliser votre propre certificat personnalisé, acheté auprès de l'autorité de certification tierce de votre choix.
- Mesures et CloudWatch surveillance intégrées : surveillez le trafic, les erreurs, le transfert de données et la latence de votre site Web.
- Protection par mot de passe : limitez l'accès à votre site Web en configurant un nom d'utilisateur et un mot de passe obligatoires dans la console Amplify.
- Redirections et réécritures : créez des règles de redirection et de réécriture dans la console Amplify pour permettre à un serveur Web de rediriger la navigation d'une URL à une autre.

Lorsque vous déployez votre application depuis un bucket Amazon S3 à usage général vers Amplify Hosting, les AWS frais sont basés sur le modèle tarifaire d'Amplify. Pour plus d'informations, consultez AWS Amplify Pricing (Tarification CTlong).

> **Important**
>
> Amplify Hosting n'est pas disponible partout Régions AWS où Amazon S3 est disponible. Pour déployer un site Web statique sur Amplify Hosting, le compartiment Amazon S3 à usage général contenant votre site Web doit être situé dans une région où Amplify est disponible. Pour obtenir la liste des régions où Amplify est disponible, consultez Points de terminaison Amplify dans le Référence générale d'Amazon Web Services.

Vous pouvez démarrer le processus de déploiement depuis la console Amazon S3, la console Amplify, la AWS CLI ou le. AWS SDKs Vous ne pouvez effectuer un déploiement sur Amplify qu'à partir d'un compartiment à usage général situé dans votre propre compte. Amplify ne prend pas en charge l'accès intercompte aux compartiments.

Utilisez les instructions suivantes pour déployer un site Web statique à partir d'un compartiment Amazon S3 à usage général vers Amplify Hosting à partir de la console Amazon S3.

Déploiement d'un site Web statique sur Amplify à partir de la console S3

Pour déployer un site Web statique à partir de la console Amazon S3

1. Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/s3/.
2. Dans le panneau de navigation de gauche, choisissez Compartiments.
3. Dans la liste Compartiments, choisissez le compartiment à usage général qui contient le site Web que vous souhaitez déployer sur Amplify Hosting.
4. Choisissez l'onglet Propriétés.
5. Sous Hébergement de site Web statique, choisissez Créer une application Amplify. À ce stade, le processus de déploiement est transféré vers la console Amplify.
6. Dans la page Déployer avec S3, procédez comme suit.
   a. Pour Nom de l'application, entrez le nom de votre application ou de votre site Web.
   b. Pour Nom de la branche, entrez le nom du côté dorsal de votre application.
   c. Pour Emplacement S3 des objets à héberger, entrez le chemin de répertoire de votre compartiment à usage général ou choisissez Parcourir S3 pour le localiser et le sélectionner.
7. Choisissez Save and deploy (Enregistrer et déployer).

> **Note**
>
> Si vous mettez à jour l'un des objets d'un site Web statique dans votre compartiment à usage général hébergé sur Amplify, vous devez redéployer l'application sur Amplify Hosting pour que les modifications prennent effet. Amplify Hosting ne détecte pas automatiquement les modifications apportées à votre compartiment. Pour plus d'informations, consultez Mise à jour d'un site Web statique déployé sur Amplify à partir d'un compartiment S3 dans le Guide de l'utilisateur AWS Amplify Hosting.

Pour démarrer directement à partir de la console Amplify, consultez Déploiement d'un site Web statique depuis S3 à l'aide de la console Amplify dans le Guide de l'utilisateur AWS Amplify Hosting.

Pour commencer à utiliser le AWS SDKs, consultez la section Création d'une politique de compartiment pour déployer un site Web statique à partir de S3 à l'aide du guide AWS SDKs de l'utilisateur d'AWS Amplify Hosting.

Marquage pour la répartition des coûts ou le contrôle d'accès basé sur les attributs (ABAC)

Une AWS balise est une paire clé-valeur qui contient des métadonnées. Vous attachez les balises à vos ressources Amazon S3, telles que des buckets. Vous pouvez étiqueter les ressources lorsque vous les créez ou gérer les balises des ressources existantes. L'utilisation de balises n'entraîne aucun frais supplémentaire au-delà des taux de requêtes standard de l'API S3. Pour plus d'informations, consultez Tarification Amazon S3.

Comment fonctionnent les tags

Amazon S3 prend en charge deux types de balises :

- AWS-tags générés : applique AWS automatiquement ces tags, et vous ne pouvez ni les modifier ni les supprimer. Pour en savoir plus sur les balises AWS générées, consultez la section Utilisation des balises AWS générées par -generated.
- Balises définies par l'utilisateur : vous appliquez ces balises à vos ressources S3 et vous les gérez.

Balises définies par l'utilisateur

Une balise définie par l'utilisateur est une paire clé-valeur de balise que vous utilisez pour étiqueter vos ressources. Les balises définies par l'utilisateur se composent d'une clé obligatoire et d'une valeur facultative. Voici les principaux composants d'une balise définie par l'utilisateur :

La clé du tag

La clé de balise correspond au nom obligatoire de la balise. Par exemple, la clé de balise `project` se trouve-t-elle dans la paire clé-valeur de balise suivante :

Clé	Valeur
`project`	`Trinity`

La clé de balise est une chaîne sensible aux majuscules et minuscules qui doit contenir entre 1 et 128 caractères Unicode. Les clés ne peuvent contenir que des lettres ou des chiffres Unicode, des espaces blancs et les symboles suivants :

- _- souligner
- .- période
- :- côlon
- /- barre oblique
- =- signe égal
- +- signe plus
- @- au panneau
- -- tiret

La valeur du tag

La valeur de la balise est une chaîne facultative. Par exemple, la valeur `Trinity` de la balise dans cette paire clé-valeur de balise est-elle :

Clé	Valeur
`project`	`Trinity`

La valeur de la balise est une chaîne sensible aux majuscules et minuscules qui peut contenir entre 0 et 256 caractères Unicode. Les valeurs ne peuvent contenir que des lettres ou des chiffres Unicode, des espaces blancs et les symboles suivants :

- _- souligner
- .- période
- :- côlon
- /- barre oblique
- =- signe égal
- +- signe plus
- @- au panneau
- -- tiret

Pour plus de détails sur les caractères autorisés dans les balises définies par l'utilisateur et sur les autres restrictions, consultez la section Restrictions relatives aux balises définies par l'utilisateur dans le guide de l'AWS Billing and Cost Management utilisateur.

Le set de tags

Chaque ressource S3 possède un ensemble de balises qui contient toutes les paires clé/valeur de balise attribuées à ce compartiment. Un jeu de balises peut être vide ou contenir jusqu'à 50 balises définies par l'utilisateur, sauf dans le cas du balisage d'objets. Les objets ne peuvent comporter que 10 balises.

Bien que chaque clé doive être unique dans un ensemble de balises, vous pouvez utiliser la même valeur plusieurs fois. Par exemple, vous pouvez avoir la même valeur pour `Trinity` les deux clés de balise suivantes :

Clé	Valeur
`project`	`Trinity`
`cost-center`	`Trinity`

Lorsque vous ajoutez une balise qui possède la même clé qu'une balise existante, la nouvelle valeur remplace l'ancienne valeur.

AWS n'applique aucune signification sémantique à vos balises. Nous interprétons les balises de façon stricte, en tant que chaîne de caractères.

Pour ajouter, répertorier, modifier ou supprimer des balises, vous pouvez utiliser la console Amazon S3, l'interface de ligne de AWS commande (AWS CLI) ou l'API Amazon S3.

Méthodes courantes d'utilisation des balises

Utilisez des balises sur vos ressources S3 pour :

1. Répartition des coûts — Suivez les coûts de stockage par compartiment AWS Billing and Cost Management.
2. Contrôle d'accès basé sur les attributs (ABAC) : adaptez les autorisations d'accès et accordez l'accès aux ressources S3 en fonction de leurs balises.

> **Note**
>
> Vous pouvez utiliser les mêmes balises pour la répartition des coûts et le contrôle d'accès.

Utilisation de balises pour la répartition des coûts

Suivez vos coûts de stockage Amazon S3 en appliquant des balises aux ressources S3 et en activant ces balises pour la répartition des coûts.

Pour commencer à suivre les coûts :

1. Ajoutez des balises à vos ressources S3 ou utilisez des balises existantes. Par exemple, vous pouvez étiqueter les buckets avec une balise identifiant un projet ou un groupe de projets.
2. Activez les balises pour la répartition des coûts dans la AWS Billing and Cost Management console. Voir Activation des balises de répartition des coûts définies par l'utilisateur dans le guide de AWS Billing and Cost Management l'utilisateur. Vous pouvez activer les balises définies ou AWS générées par l'utilisateur. Pour plus d'informations, voir Organisation et suivi des coûts à l'aide de balises de répartition des AWS coûts.

AWS utilise les balises activées pour organiser vos coûts de ressources dans divers outils de facturation et de gestion des coûts, tels que :

- Rapport de répartition des coûts

  Fournit une vue globale des coûts organisés en fonction de vos balises activées. Pour plus d'informations, consultez la section Utilisation du rapport mensuel de répartition des coûts dans le Guide AWS de l'utilisateur de facturation.
- Rapport sur les coûts et l'utilisation (CUR)

  Fournit l'ensemble le plus détaillé de données sur les AWS coûts et l'utilisation, y compris des ventilations des coûts basées sur des balises. Pour plus d'informations, voir Que sont les rapports de AWS coûts et d'utilisation ? dans le Guide de l'utilisateur de AWS Data Export.

Ressources Amazon S3 qui prennent en charge les coûts de suivi à l'aide de balises

Les ressources Amazon S3 suivantes prennent en charge le suivi des coûts de stockage à l'aide de balises.

- Compartiments de répertoire

  Pour plus d'informations, consultez la section Gestion des balises pour les compartiments de répertoire.
- Seaux à usage général

  Pour plus d'informations, consultez la section Gestion des balises pour les compartiments à usage général.

Utilisation de balises pour le contrôle d'accès basé sur les attributs (ABAC)

Le contrôle d'accès basé sur les attributs (ABAC) est une stratégie d'autorisation qui définit les autorisations en fonction des attributs, c'est-à-dire des balises. Vous pouvez associer des balises à des entités AWS Identity and Access Management (IAM) (utilisateurs ou rôles) et à des AWS ressources, telles que les points d'accès Amazon S3 et les compartiments d'annuaire. Vous contrôlez ensuite les autorisations d'accès à ces ressources à l'aide de conditions basées sur des balises dans les politiques de contrôle d'accès afin d'autoriser ou de refuser les opérations lorsque ces conditions sont remplies.

Avec ABAC, vous utilisez des clés de condition basées sur des balises dans vos AWS organisations, IAM et les politiques de ressources S3. Pour les entreprises, l'ABAC d'Amazon S3 prend en charge l'autorisation sur plusieurs AWS comptes.

Dans vos politiques IAM, vous pouvez contrôler l'accès aux ressources S3 en fonction des balises du compartiment à l'aide de clés de condition.

Clés de condition prises en charge

Vous pouvez utiliser les clés de AWS condition suivantes pour toutes les ressources Amazon S3 compatibles avec ABAC.

- `aws:ResourceTag/key-name`
- `aws:RequestTag/key-name`
- `aws:TagKeys`

Certaines ressources prennent en charge des clés de condition Amazon S3 supplémentaires. Pour obtenir la liste complète des clés de condition pouvant être utilisées pour ABAC et des exemples de politiques, consultez les rubriques de balisage suivantes relatives à la ressource.

Ressources Amazon S3 compatibles avec ABAC

Les ressources Amazon S3 suivantes prennent en charge le contrôle d'accès basé sur les attributs (ABAC) à l'aide de balises.

- Points d'accès

  Pour plus d'informations, consultez Utilisation de balises avec des points d'accès S3 pour des compartiments à usage général et Utilisation de balises avec des points d'accès S3 pour les compartiments de répertoire.
- Tâches liées aux opérations par lots

  Pour de plus amples informations, veuillez consulter Contrôle de l'accès et étiquetage des tâches à l'aide d'étiquettes.
- Compartiments de répertoire

  Pour de plus amples informations, veuillez consulter Utilisation de balises avec des compartiments de répertoire S3.
- Objets

  Pour de plus amples informations, veuillez consulter Catégorisation de vos objets à l'aide de balises.
- Subventions d'accès S3

  Pour de plus amples informations, veuillez consulter Gestion des balises pour les subventions d'accès S3.
- Groupes de lentilles de stockage S3

  Pour de plus amples informations, veuillez consulter Gestion des balises de AWS ressources avec les groupes Storage Lens.

Planification de votre stratégie de marquage

Nous vous recommandons de concevoir un ensemble de clés d'étiquette répondant à vos besoins pour chaque type de ressource. L'utilisation d'un ensemble de clés de balise cohérent facilite la gestion de vos ressources. Vous pouvez rechercher et filtrer les ressources en fonction des étiquettes que vous ajoutez. Pour plus d'informations sur la mise en œuvre d'une stratégie de balisage des ressources efficace, consultez le livre blanc sur les meilleures pratiques AWS en matière de balisage.

Bonnes pratiques pour le balisage des ressources Amazon S3

Lorsque vous utilisez des balises, nous vous recommandons de suivre les bonnes pratiques suivantes :

- Documentez les conventions relatives à l'utilisation des balises qui sont suivies par toutes les équipes de votre organisation. Assurez-vous notamment que les noms sont à la fois descriptifs et cohérents. Par exemple, normalisez le format `environment:prod` plutôt que d'étiqueter certaines ressources avec. `env:production`

  > **Important**
  >
  > Ne stockez pas d'informations personnelles identifiables (PII) ou d'autres informations confidentielles ou sensibles dans des balises.

- Automatisez le balisage pour garantir la cohérence. Par exemple, vous pouvez inclure des balises dans un AWS CloudFormation modèle. Lorsque vous créez des ressources à l'aide du modèle, elles sont étiquetées automatiquement.
- N'utilisez des balises que lorsque cela est nécessaire. Évitez la prolifération et la complexité inutiles des balises.
- Vérifiez régulièrement la pertinence et l'exactitude des balises. Supprimez ou modifiez les balises obsolètes selon vos besoins.
- Envisagez de créer des balises à l'aide de l'éditeur de AWS balises de la console AWS de gestion. Vous pouvez utiliser l'éditeur de balises pour ajouter des balises à plusieurs AWS ressources prises en charge, y compris les ressources Amazon S3, en même temps. Pour plus d'informations, consultez la section Tag Editor dans le Guide de l'utilisateur d'AWS Resource Groups.

Gestion des balises pour les ressources Amazon S3

Pour plus d'informations sur la gestion des balises pour les ressources Amazon S3, consultez les pages suivantes :

- Gestion des balises pour les points d'accès pour les buckets à usage général
- Gestion des balises pour les points d'accès pour les compartiments d'annuaire
- Contrôle de l'accès et étiquetage des tâches à l'aide d'étiquettes
- Gestion des balises pour les compartiments de répertoires

- Gestion des balises pour les compartiments à usage général
- Catégorisation de vos objets à l'aide de balises
- Gestion des balises pour les subventions d'accès S3
- Gestion des balises de AWS ressources avec les groupes Storage Lens

Quotas

Vous Compte AWS disposez de quotas par défaut, anciennement appelés limites, pour chaque AWS service. Les quotas Amazon S3 comprennent le nombre de compartiments à usage général, de compartiments de répertoires, de points d'accès, etc. Vous pouvez demander une augmentation de certains quotas, mais tous les quotas ne peuvent pas être augmentés. Ces augmentations ne sont pas accordées immédiatement, plusieurs jours peuvent être nécessaires pour que votre augmentation soit effective.

Pour obtenir la liste des quotas Amazon S3 et de leurs valeurs par défaut, consultez Quotas Amazon S3 dans la Références générales AWS.

Augmentations des quotas

Pour demander une augmentation de quota

Vous pouvez demander une augmentation de quota en utilisant l'une des options suivantes :

- À partir de AWS Management Console : Ouvrez la console Service Quotas. Dans le volet de navigation, choisissez Services AWS . Sélectionnez Amazon S3, sélectionnez un quota et suivez les instructions pour demander une augmentation de quota. Pour accéder aux instructions, consultez Requesting a quota increase dans le Guide de l'utilisateur Service Quotas.
- À partir de AWS CLI : Utilisez la request-service-quota-increase AWS CLI commande. Pour accéder aux instructions, consultez Requesting a quota increase dans le Guide de l'utilisateur Service Quotas.

Référence

Outre la console Amazon S3, vous pouvez travailler avec Amazon S3 par programmation à l'aide du REST APIs AWS SDKs, ou AWS Command Line Interface ()AWS CLI d'Amazon S3.

- Référence des API Amazon Simple Storage Service
- Exemples de code dans la Référence d'API Amazon Simple Storage Service
- AWS Interface de ligne de commande dans le guide de AWS Command Line Interface l'utilisateur.
- AWS SDKs

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 pour des exemples PowerShell de code
AWS SDK pour Python (Boto3)	AWS SDK pour Python (Boto3) exemples de code
AWS SDK pour Ruby	AWS SDK pour Ruby exemples de code
Kit AWS SDK pour Rust	Kit AWS SDK pour Rust exemples de code
AWS SDK pour SAP ABAP	AWS SDK pour SAP ABAP exemples de code

Documentation SDK	Exemples de code
Kit AWS SDK pour Swift	Kit AWS SDK pour Swift exemples de code

Historique du document

- Version de l'API actuelle : 2006-03-01

La table suivante décrit les modifications importantes apportées à chaque version de la Référence d'API Amazon Simple Storage Service et du Guide de l'utilisateur Amazon S3. Pour recevoir les notifications de mise à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Amazon S3 prend désormais en charge les balises Access Points pour le contrôle d'accès basé sur les attributs (ABAC)	Amazon S3 prend désormais en charge le balisage des points d'accès à la fois pour un usage général et pour les compartiments d'annuaire. Ajoutez des balises aux points d'accès et utilisez le contrôle d'accès basé sur les attributs (ABAC) pour étendre l'accès. Vous pouvez commencer à baliser les points d'accès à l'aide de la console AWS de gestion, de l'API REST S3, de la AWS CLI ou du AWS SDK. Pour en savoir plus sur l'utilisation des balises pour ABAC, consultez la section Utilisation des balises pour le contrôle d'accès basé sur les attributs (ABAC).	31 juillet 2025
Vecteurs Amazon S3 (version préliminaire)	Amazon S3 Vectors fournit un stockage vectoriel spécialement conçu et optimisé en termes de coûts pour vos applications de recherche	15 juillet 2025

sémantique et d'intelligence artificielle. S3 Vectors introduit un nouveau type de compartiment, le bucket vectoriel, optimisé pour un stockage vectoriel durable et peu coûteux. Pour plus d'informations, consultez la section Utilisation des vecteurs S3 et des buckets vectoriels.

Les métadonnées Amazon S3 prennent désormais en charge les objets existants	Amazon S3 Metadata crée et gère des métadonnées qui fournissent des informations sur les ensembles de données stockés dans S3, afin que vous puissiez découvrir et utiliser plus facilement vos données S3. Auparavant, les métadonnées S3 prenaient en charge les objets nouveaux et mis à jour. Désormais, S3 Metadata crée et gère également les métadonné es pour toutes vos données S3 existantes. S3 Metadata crée et gère désormais deux Apache Iceberg tables qui vous fournissent une vue interrogeable et continuel lement mise à jour des métadonnées associées aux objets d'un compartiment à usage général. Un tableau de journal enregistre les modifications apportées à vos données en temps quasi réel, ce qui vous aide à identifie r les nouvelles données téléchargées dans votre compartiment, à suivre les objets récemment supprimés , à surveiller les transitions du cycle de vie S3, etc. Un nouveau tableau d'inventa ire en temps réel fournit et conserve une up-to-date vue	15 juillet 2025

de tous les objets de votre compartiment. Les deux tables de métadonnées S3 sont stockées dans un compartiment de tables Iceberg AWS géré de votre compte et peuvent être consultées à l'aide du SQL standard via des services AWS d'analyse, tels qu'Amazon Athena ou Amazon EMR, et des outils open source, tels que et. DuckDB PyIceberg Pour plus d'informations, consultez Accélération de la découverte des données avec les métadonnées S3.

Amazon S3 Express One Zone prend désormais en charge les balises pour la répartition des coûts et le contrôle d'accès basé sur les attributs	Amazon S3 Express One Zone, une classe de stockage S3 à hautes performances, prend désormais en charge les balises pour la répartition des coûts et le contrôle d'accès basé sur les attributs (ABAC). Vous pouvez ajouter des balises aux compartiments du répertoire S3 pour suivre et organiser les AWS coûts à l'aide AWS Billing and Cost Management de. En outre, grâce à la prise en charge de l'ABAC, vous pouvez étendre le contrôle d'accès à vos compartiments d'annuaire à l'aide de balises. S3 Express One Zone prend en charge les balises sur les compartiments de répertoire dans tous Région AWS les emplacements où la classe de stockage est disponible. Vous pouvez commencer à utiliser le balisage à l'aide de la console AWS de gestion, de l'API REST S3, de la AWS CLI ou du AWS SDK. Pour en savoir plus sur l'utilisation de balises pour simplifier la répartition des coûts ou ABAC, consultez la section Utilisation de balises avec des compartiments de répertoire S3.	2 juillet 2025

Les points d'accès prennent désormais en charge l'attachement à un FSx volume pour OpenZFS	Vous pouvez créer et associer un point d'accès à un volume FSx pour OpenZFS à l'aide de FSx la console Amazon ou de l' AWS CLI API. Une fois attaché, vous pouvez utiliser l'objet S3 APIs pour accéder aux données de votre fichier. Vos données continuent de résider dans le système de FSx fichiers Amazon et d'être directement accessibles pour vos charges de travail existantes. Pour plus d'informations, consultez la section Gestion de l'accès aux ensembles de données partagés avec des points d'accès.	25 juin 2025
S3 Tables prend désormais en charge de nouvelles stratégies de compactage pour les tables	S3 Tables prend désormais en charge plusieurs stratégies de compactage afin d'optimiser les performances des requêtes en fonction des différents modèles d'accès aux données. Les nouvelles stratégies incluent le tri et l'ordre Z. Pour plus d'informations, consultez la section Stratégies de compactage pour les tables.	18 juin 2025

S3 Tables ajoute une nouvelle politique AWS gérée pour les tables S3	S3 Tables a ajouté une nouvelle politique AWS gérée appeléeAmazonS3T ablesLakeFormation ServiceRole . Cette politique accorde des autorisat ions qui permettent au rôle de service Lake Formation d'accéder aux tables et aux compartiments de tables Amazon S3. Pour plus d'informations, consultez les politiques AWS gérées pour les tables S3.	19 mai 2025
S3 Tables prend désormais en charge le SSE-KMS à l'aide de clés gérées par le client	S3 Tables prend désormais en charge le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) à l'aide de clés gérées par le client. Vous pouvez appliquer le chiffrement SSE-KMS au niveau du bucket et de la table. Pour plus d'informa tions, consultez la section Utilisation du chiffrement côté serveur avec des AWS KMS clés (SSE-KMS) dans des compartiments de table.	16 avril 2025

Les points d'accès pour les compartiments de répertoire sont disponibles dans les Zones AWS Locales	Les compartiments d'annuaire prennent désormais en charge les points d'accès afin de simplifier la gestion de l'accès aux données à grande échelle pour les ensembles de données partagés dans Amazon S3. Grâce à cette nouvelle fonctionnalité, vous pouvez créer des centaines de points d'accès par compartiment, chacun ayant un nom distinct et des autorisations personnalisées pour chaque application. Pour plus d'informations, consultez la section Gestion de l'accès aux ensembles de données partagés dans des compartiments de répertoire dotés de points d'accès.	31 mars 2025

L'intégration du bucket de table S3 à Amazon SageMaker Lakehouse est désormais disponible pour tous	Vous pouvez intégrer des compartiments de tables S3 à Amazon SageMaker Lakehouse pour accéder aux tables à partir de services AWS d'analyse, tels qu'Amazon Athena, Amazon Redshift et. QuickSigh t Amazon SageMaker Lakehouse unifie vos données entre les lacs de données Amazon S3 et les entrepôts de données Amazon Redshift, afin que vous puissiez créer des applications d'analyse , d'apprentissage automatiq ue (ML) et d'IA générativ e sur une seule copie des données. L'intégration remplit les ressources AWS Glue Data Catalog de votre table et fédère l'accès à ces ressources avec. AWS Lake Formation L'intégration permet un contrôle d'accès précis via Lake Formation afin de renforcer la sécurité. Pour plus d'informations sur l'intégration, consultez la section Utilisation des tables Amazon S3 avec les services AWS d'analyse. Si vous avez configuré l'intégra tion avec la version prélimina ire, vous pouvez continuer à utiliser votre intégration actuelle. Cependant, le	13 mars 2025

	processus d'intégration mis à jour permet d'améliorer les performances. Nous vous recommandons donc de procéder à la migration. Pour migrer vers l'intégration mise à jour, consultez la section Migration vers le processus d'intégration mis à jour.	
Les tables S3 créent un support de table et de table de requête ajouté à la console Amazon S3	Les tables S3 prennent désormais en charge les opérations de création de table et de table de requête directement depuis la console Amazon S3 à l'aide d'Amazon Athena. Grâce à cette nouvelle fonctionnalité, vous pouvez désormais créer une table, la remplir de données et l'interroger en quelques étapes dans la console Amazon S3. Pour plus d'informations, consultez Création d'une table Amazon S3 et Interrogation de tables Amazon S3 avec Athena.	13 mars 2025
S3 Tables ajoute la prise en charge de l'ajout de schémas lors de la création de tables	Vous pouvez désormais utiliser l'opération d'`CreateTable` API S3 Tables pour créer des tables avec des schémas en ajoutant un indicateur de métadonnées facultatif. Pour plus d'informations, consultez la section Création de tables.	30 janvier 2025

S3 Tables ajoute la prise en charge de l'ajout de schémas lors de la création de tables	Vous pouvez désormais utiliser l'opération d'`CreateTable` API S3 Tables pour créer des tables avec des schémas en ajoutant un indicateur de métadonnées facultatif. Pour plus d'informations, consultez la section Création de tables.	30 janvier 2025

Les métadonnées S3 sont désormais disponibles pour tous	Les métadonnées Amazon S3 sont désormais disponibles pour tous. Les métadonnées S3 vous aident à découvrir et à comprendre facilement vos données S3 grâce à des métadonnées automatisées et interrogeables qui sont mises à jour quasiment en temps réel. Avec S3 Metadata, vous pouvez organiser, identifier et utiliser vos données S3 pour l'analyse commerciale, l'apprentissage de modèles d'intelligence artificielle et d'apprentissage automatique (AI/ML), etc. Les métadonnées S3 prennent en charge les métadonnées d'objet, qui incluent des informations définies par le système telles que la taille et la source de l'objet, et des métadonnées personnalisées, telles que des balises contenant des informations telles que les évaluations du produit SKUs, des transactions IDs ou du contenu. Pour plus d'informations, consultez Accélération de la découverte des données avec les métadonnées S3.	27 janvier 2025
Politiques gérées par AWS : nouvelles politiques	S3 Tables a ajouté deux nouvelles politiques AWS gérées.	6 décembre 2024

Tableaux S3	Amazon S3 Tables fournit un stockage S3 optimisé pour les charges de travail analytiques, avec des fonctionnalités qui améliorent les performances des requêtes, réduisent les coûts de stockage des tables et simplifient le fonctionnement des lacs de données à grande échelle. S3 Tables introduit un nouveau type de compartiment : les compartiments de table, spécialement conçus pour stocker Apache Iceberg des tables en tant que sous-ressources. Les compartiments de tables offrent un plus grand nombre de transactions par seconde (TPS) et un meilleur débit de requêtes par rapport aux tables autogérées dans les compartiments S3 à usage général. Vous pouvez intégrer automatiquement vos compartiments de table à des services AWS d'analyse tels qu'Athena, Amazon QuickSight Redshift, etc. Pour plus d'informations, consultez la section Utilisation des tables et des compartiments de tables Amazon S3.	3 décembre 2024

Aperçu des métadonnées S3	Amazon S3 Metadata vous permet de découvrir et de comprendre facilement vos données S3 grâce à des métadonnées automatisées et interrogeables qui sont mises à jour quasiment en temps réel. Avec S3 Metadata, vous pouvez organiser, identifier et utiliser vos données S3 pour l'analyse commerciale, l'apprentissage de modèles d'intelligence artificielle et d'apprentissage automatique (AI/ML), etc. Les métadonnées S3 prennent en charge les métadonnées d'objet, qui incluent des informations définies par le système telles que la taille et la source de l'objet, et des métadonnées personnalisées, telles que des balises contenant des informations telles que les évaluations du produit SKUs, des transactions IDs ou du contenu. Pour plus d'informations, consultez Accélération de la découverte des données avec les métadonnées S3.	3 décembre 2024

Navigateur de stockage pour S3	Le navigateur de stockage pour S3 est un composant open source que vous pouvez ajouter à vos applications web afin de fournir à vos utilisate urs finaux une interface simple pour les données stockées dans S3. Pour plus d'informa tions, consultez Navigateur de stockage pour S3.	1er décembre 2024
Nouvel algorithme de somme de contrôle Amazon S3 et fonctionnalités améliorées d'intégrité des sommes de contrôle	Amazon S3 ajoute l'algorit hme de somme de contrôle `CRC-64NVME` et les fonctionn alités améliorées d'intégrité des sommes de contrôle. Pour plus d'informations, consultez Vérification de l'intégrité des objets dans Amazon S3.	1er décembre 2024
Charges de travail liées à la résidence des données	Dans les zones locales dédiées, vous pouvez créer des compartiments de répertoires S3 pour stocker les données pour vos cas d'utilisation liés à la résidence et à l'isolement des données. Pour plus d'informations, consultez la section Charges de travail liées à la résidence des données.	1er décembre 2024

Nouvelles clés de condition pour appliquer les écritures conditionnelles	Amazon S3 ajoute les nouvelles clés de condition `s3:if-match` et `s3:if-none-match` à utiliser dans les politiques de compartiments pour obliger les clients à utiliser l'en-tête HTTP `If-None-Match` ou `If-Match`. Pour plus d'informations, consultez Application d'écritures conditionnelles sur des compartiments Amazon S3.	25 novembre 2024
Nouvel en-tête HTTP pour les écritures conditionnelles afin de vérifier si l'objet a changé	Amazon S3 ajoute l'en-tête `If-Match` HTTP pour vérifier la balise d'entité (ETag) d'un objet avant d'écrire un objet pour certaines opérations d'API. Avec cet en-tête, Amazon S3 compare la ETag valeur fournie avec la ETag valeur de l'objet dans S3. Si les ETag valeurs ne correspondent pas, l'opération échoue. Pour plus d'informations, consultez Comment empêcher le remplacement d'objets par des écritures conditionnelles.	25 novembre 2024

Amazon Redshift s’intègre désormais aux autorisations d’accès S3	Les clients Amazon Redshift peuvent désormais utiliser les autorisations d’accès S3 pour mettre à l’échelle et gérer les autorisations pour leurs données S3. Cela permet aux clients d'Amazon Redshift de dimensionner les autorisations S3 pour les identités d'entreprise en utilisant AWS IAM Identity Center et pour les utilisate urs et les groupes IAM. Pour plus d’informations, consultez Intégration d’Amazon Redshift aux autorisations d’accès Amazon S3.	15 novembre 2024
AWS Organizations les comptes membres peuvent désormais accéder de nouveau aux compartim ents Amazon S3 verrouillés accidentellement	AWS Organizations les comptes membres peuvent désormais utiliser un processus simple AWS Identity and Access Management (IAM) pour retrouver l'accès aux compartiments Amazon S3 verrouillés accidentellement. Pour plus d'informations, voir Exécuter une tâche privilégiée sur un compte AWS Organizat ions membre dans le Guide de AWS Identity and Access Management l'utilisateur.	14 novembre 2024

Les politiques de contrôle des ressources (RCPs), un nouveau type de politique d'autorisation AWS Organizations est également disponible pour les compartiments Amazon S3	Politiques de contrôle des ressources (RCPs), une nouvelle politique d'autorisation gérée dans AWS Organizations peut être utilisée pour définir le maximum d'autorisations disponibles sur les compartiments Amazon S3 au sein de l'ensemble de votre organisation. Pour plus d'informations, voir Politiques de contrôle des ressources (RCPs) dans le guide de AWS Organizations l'utilisateur.	13 novembre 2024
Amazon S3 approuve désormais automatiquement les augmentations de quota de compartiments jusqu'à 1 000 compartiments	Amazon S3 approuve désormais automatiquement les augmentations de quota de compartiments jusqu'à 1 000 compartiments. Pour consulter l'utilisation de vos compartiments ou demander une augmentation, accédez à la console Service Quotas.	30 septembre 2024

Nouveau comportement de transition par défaut de la taille minimale des objets pour les configurations du cycle de vie Amazon S3	Amazon S3 applique désormais un comportement par défaut aux configurations du cycle de vie S3, qui empêche la transition des objets de moins de 128 Ko vers toute classe de stockage. Pour découvrir comment remplacer ce comportement, consultez Permettre la transition d'objets de moins de 128 Ko.	24 septembre 2024
Les compartiments de répertoires prennent désormais en charge SSE-KMS à l'aide de clés gérées par le client.	Les compartiments d'annuaire prennent désormais en charge le chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) à l'aide de clés gérées par le client. Vous disposez d'autres options pour chiffrer et gérer la sécurité de vos données dans des compartiments de répertoires. Pour plus d'informations, consultez Protection et chiffrement des données dans des compartiments de répertoires.	17 septembre 2024

Les autorisations d'accès S3 prennent en charge une action d'API qui répertorie les autorisations d'accès de l'appelant	Les identités IAM et les identités d'annuaire IAM Identity Center peuvent désormais utiliser l'API `ListCallerAccessGrants` pour répertorier tous les compartiments, préfixes et objets Amazon S3 auxquels elles peuvent accéder, tels que définis par leurs autorisations d'accès S3. Utilisez cette API pour découvrir toutes les données S3 auxquelles une identité IAM ou une identité d'annuaire d'entreprise peut accéder via les autorisations d'accès S3, au sein d'un Compte AWS particulier. Pour plus d'informations, consultez Répertorier les autorisations d'accès de l'appelant.	5 septembre 2024

Messages d'erreur de refus d'accès améliorés pour les demandes portant sur le même compte	Amazon S3 inclut désormais un contexte supplémentaire dans les erreurs de refus d'accès (HTTP `403 Forbidden`) pour les demandes adressées aux ressources du même Compte AWS. Ce nouveau contexte inclut le type de politique qui a refusé l'accès, le motif du refus et les informations sur l'utilisateur ou le rôle AWS Identity and Access Management (IAM) qui a demandé l'accès à la ressource. Ce contexte vous aide à résoudre les problèmes d'accès, à identifier la cause première des erreurs de refus d'accès et à corriger les contrôles d'accès incorrects en mettant à jour les politiques pertinentes. Ce contexte supplémentaire est également disponible dans les AWS CloudTrail journaux. Les messages d'erreur de refus d'accès améliorés pour les demandes portant sur le même compte sont désormais disponibles dans toutes les régions Régions AWS, y compris en Chine AWS GovCloud (US) Regions et en Chine. Pour plus d'informations, consultez Résolution des erreurs d'accès	21 août 2024

	refusé (403 Forbidden) dans Amazon S3.	
Amazon S3 prend en charge l'utilisation d'écritures conditionnelles pour `PutObject` et `CompleteMultipartUpload`	Vous pouvez vérifier l'existence d'un objet dans un compartiment avant de le créer à l'aide d'une écriture conditionnelle lors des opérations de chargement. Cela permet d'éviter l'écrasement de données existantes. Les écritures conditionnelles valident qu'aucun objet portant le même nom de clé ne se trouve déjà dans votre compartiment. Pour plus d'informations, consultez Demandes conditionnelles.	20 août 2024
Amazon S3 ne facture plus pour plusieurs codes d'erreur HTTP	Amazon S3 a effectué une modification afin que les demandes non autorisées que les clients n'ont pas initiées soient gratuites. Pour plus d'informations, consultez Facturation des réponses d'erreur Amazon S3.	19 août 2024
Amazon S3 Select n'est plus disponible pour les nouveaux clients	Amazon S3 Select n'est plus disponible pour les nouveaux clients. Les clients existants d'Amazon S3 Select peuvent continuer à utiliser cette fonctionnalité comme d'habitude. En savoir plus.	25 juillet 2024

Amazon S3 Inventory prend en charge la clé de Inventory AccessibleOptionalFields condition s3 :	Amazon S3 Inventory prend en charge la clé de Inventory AccessibleOptionalFields condition s3 : pour contrôler si les utilisateurs peuvent inclure des champs de métadonnées facultatifs dans leurs rapports. Pour plus d'informations, consultez Contrôle de la création de la configuration des rapports d'inventaire S3.	20 février 2024
IPv6 support pour S3 sur Outposts	Vous pouvez désormais accéder à S3 sur les compartiments Outposts en utilisant les points de terminaison à double pile IPv6 via S3 on Outposts. IPv6 le support de S3 on Outposts vous permet de gérer vos buckets S3 on Outposts et les ressources du plan de contrôle sur les réseaux. IPv6	16 janvier 2024
Nouvelle classe de stockage Amazon S3 à zone unique et hautes performances : S3 Express One Zone	Amazon S3 Express One Zone est une classe de stockage Amazon S3 à zone unique et hautes performan ces, spécialement conçue pour fournir un accès aux données constant en moins de dix millisecondes pour vos applications les plus sensibles à la latence. Pour plus d'informations, consultez S3 Express One Zone.	28 novembre 2023

Mountpoint pour Amazon S3 ajoute la prise en charge de S3 Express One Zone	Vous pouvez désormais monter des compartiments de répertoires S3 Express One Zone avec Mountpoint.	28 novembre 2023
Version du schéma d'invocation Lambda	Les opérations par lots Amazon S3 introduisent une nouvelle version du schéma d'invocation Lambda à utiliser avec les tâches d'opérations par lots qui agissent sur des compartiments de répertoires. Pour plus d'informations, consultez Utilisation de Lambda et des opérations par lots Amazon S3 avec des compartiments de répertoires.	28 novembre 2023
Action d'importation pour les compartiments de répertoires	Amazon S3 introduit l'action d'importation. L'importation est une méthode simplifiée pour créer des tâches d'opérations par lots Amazon S3 afin de copier des objets depuis des compartiments à usage général vers des compartiments de répertoires. Pour plus d'informations, consultez Importation d'objets dans un compartiment de répertoires.	28 novembre 2023

Gestion des accès S3 avec les autorisations d'accès S3	Les autorisations d'accès Amazon S3 vous permettent de gérer les autorisations de données à grande échelle pour les principaux AWS Identity and Access Management (IAM), en plus des identités d'annuaire issues des annuaires d'entreprise tels qu'Azure AD. Vous pouvez désormais appliquer les autorisations S3 de moindre privilège et facilement adapter ces autorisations en fonction des besoins de votre entreprise. Pour plus d'informations, consultez Gestion de l'accès avec les octrois d'accès S3.	26 novembre 2023
Mountpoint pour Amazon S3 ajoute une fonctionnalité de mise en cache	Avec Mountpoint, vous pouvez désormais configurer la mise en cache pour les données consultées à plusieurs reprises.	22 novembre 2023

Génération améliorée du manifeste d'opérations par lot Amazon S3	Vous pouvez désormais indiquer aux opérations par lots Amazon S3 de générer automatiquement un manifeste en fonction des critères de filtre d'objet que vous spécifiez lors de la création de votre tâche. Cette option est disponible pour les tâches de réplication par lots que vous créez dans la console Amazon S3, ou pour tout type de tâche que vous créez à l'aide de l'API REST AWS CLI AWS SDKs, ou Amazon S3. Pour plus d'informations, consultez Création d'une tâche d'opérations par lots Amazon S3.	22 novembre 2023
Les compartiments Amazon S3 existants peuvent désormais ajouter des configurations de verrouillage d'objet	Vous pouvez désormais activer le verrouillage d'objet sur le compartiment Amazon S3 existant. Vous pouvez définir des conservations légales et des périodes de rétention pour les compartiments nouveaux ou existants. Pour plus d'informations, consultez Utilisation du verrouillage des objets.	20 novembre 2023

Métriques de demande S3 Storage Lens pour les préfixes	S3 Storage Lens introduit les métriques de demande pour les préfixes au sein d'un compartiment Amazon S3. Pour plus d'informations, consultez Catégories de métriques.	17 novembre 2023
Groupes Amazon S3 Storage Lens	S3 Storage Lens introduit les groupes Storage Lens, un filtre défini personnalisé pour les objets basé sur les métadonnées des objets. Pour plus d'informations, consultez Utilisation des groupes Amazon S3 Storage Lens.	15 novembre 2023
Nouvelle politique IAM	S3 sur Outposts introduit `AWSServiceRoleForS3OnOutposts` , rôle lié à un service destiné à vous faciliter la gestion des ressources réseau. Pour en savoir plus, consultez Utilisation de rôles liés à un service pour S3 sur Outposts.	3 octobre 2023
Amazon S3 indique l'heure `Last-Modified` pour les marqueurs de suppression	Amazon S3 indique l'heure `Last-Modified` des marqueurs de suppression dans les en-têtes de réponse des opérations `Head` et `Get` de S3 et de l'API, respectiv ement. Pour en savoir plus, consultez Utilisation des marqueurs de suppression.	27 septembre 2023

Amazon S3 : mise à jour de la politique AWS gérée	Amazon S3 a ajouté des autorisations `s3:Describe*` à `AmazonS3ReadOnlyAccess`. Pour plus d'informations, consultez Politiques gérées par AWS pour Amazon S3.	11 août 2023
Temps de démarrage améliorés pour les demandes de restauration standard effectuées via les opérations par lot S3	Les récupérations standard pour les demandes de restauration effectuées via les opérations par lot S3 peuvent désormais démarrer en quelques minutes. Pour plus d'informations, consultez Options de récupération des archives.	9 août 2023
Ajout de Mountpoint, un client à haut débit permettant de monter un compartiment Amazon S3 en tant que système de fichiers local.	Avec Mountpoint, vos applications peuvent accéder aux objets stockés dans Amazon S3 par le biais d'opérations sur les fichiers, ce qui leur permet d'accéder au stockage et au débit élastiques d'Amazon S3 via une interface de fichier.	9 août 2023

Chiffrement double couche côté serveur avec AWS Key Management Service clés (DSSE-KMS)	Le chiffrement double couche côté serveur avec des clés AWS Key Management Service (AWS KMS) (DSSE-KMS) applique deux couches de chiffrement aux objets lorsqu'ils sont chargés sur Amazon S3. Pour plus d'informations, consultez la section Utilisation du chiffrement double couche côté serveur avec des clés. AWS KMS	13 juin 2023
Amazon S3 active l'accès public par blocs S3 et désactive les listes de contrôle d'accès S3 (ACLs) pour tous les nouveaux compartiments.	Amazon S3 active désormais automatiquement l'accès public aux blocs S3 et désactive les listes de contrôle d'accès S3 (ACLs) pour tous les nouveaux compartiments S3 dans toutes les AWS régions. Pour plus d'informations, consultez Blocage de l'accès public à votre espace de stockage Amazon S3, Contrôle de la propriété des objets et désactivation ACLs de votre compartiment.	27 avril 2023
Métrique d'échec des opérations de réplication S3	Amazon S3 ajoute une nouvelle Amazon CloudWatch métrique pour surveiller les échecs de réplication S3. Pour plus d'informations, consultez Surveillance de l'avancement des métriques de réplication.	5 avril 2023

DNS privé	AWS PrivateLink pour Amazon S3 prend désormais en charge le DNS privé. Pour plus d'informations, consultez Private DNS (DNS privés).	14 mars 2023
Prise en charge des points d'accès intercompte dans la console Amazon S3	Amazon S3 prend désormais en charge la création de points d'accès intercompte à l'aide de la console Amazon S3. Pour plus d'informations, consultez Création de points d'accès.	14 mars 2023
Amazon S3 sur Outposts prend en charge la réplication S3 sur Outposts	Avec la réplication S3 locale, vous pouvez automatiquement répliquer des objets vers un compartiment de destination Outposts unique ou plusieurs compartiments de destination. Les compartiments de destination peuvent se trouver dans des Outposts différents AWS Outposts ou dans les mêmes Outposts que le compartiment source. Pour plus d'informations, consultez Replicating objects for S3 sur Outposts (Réplication d'objets pour S3 sur Outposts).	14 mars 2023

Alias des points d'accès Amazon S3 Object Lambda	Quand vous créez un point d'accès Object Lambda, Amazon S3 génère automatiquement un alias unique pour votre point d'accès Object Lambda. Vous pouvez utiliser cet alias à la place d'un nom de compartiment Amazon S3 ou de l'Amazon Resource Name (ARN) du point d'accès Object Lambda dans une demande pour les opérations de plan de données de point d'accès. Pour plus d'informations, consultez How to use a bucket-style alias for your Object Lambda Access Point (Comment utiliser un alias de type compartiment pour votre point d'accès Object Lambda).	14 mars 2023
Prise en charge des points d'accès multi-régions intercomptes d'Amazon S3	Amazon S3 prend désormais en charge la création de points d'accès multirégions intercomptes à l'aide de la console Amazon S3. Pour plus d'informations, consultez Création de points d'accès multi-Régions.	14 mars 2023

Points d'accès intercompte	Amazon S3 prend en charge la création de points d'accès intercompte. Vous pouvez créer un point d'accès intercompte en utilisant l'opération AWS Command Line Interface (AWS CLI) ou l'opération d'API REST `CreateAccessPoint` . Pour plus d'informations, consultez Création de points d'accès.	30 novembre 2022
Amazon S3 prend en charge les contrôles de basculement pour les points d'accès multi-régions d'Amazon S3	Amazon S3 introduit le contrôle du basculement pour les points d'accès multi-régions. Ces contrôles vous permettent de déplacer le trafic des requêtes d'accès aux données S3 acheminées par un point d'accès multi-régions Amazon S3 vers une autre Région AWS en quelques minutes pour tester et créer des applications hautement disponibles. Pour plus d'informations, consultez Contrôles du basculement du point d'accès multi-régions d'Amazon S3.	28 novembre 2022

Amazon S3 Storage Lens améliore la visibilité de l'organisation grâce à 34 nouvelles métriques	S3 Storage Lens introduit 34 métriques supplémentaires pour découvrir des opportunités d'optimisation des coûts plus approfondies, identifier les bonnes pratiques de protection des données et améliorer les performances des flux d'applications. Pour plus d'informations, consultez S3 Storage Lens metrics (Métriques S3 Storage Lens).	17 novembre 2022
Amazon S3 prend en charge des taux de demande de restauration plus élevés pour S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive	Amazon S3 prend en charge les demandes de restauration à un taux pouvant atteindre 1 000 transactions par seconde, Compte AWS pour les classes de stockage S3 Glacier Flexible Retrieval et S3 Glacier Deep Archive.	15 novembre 2022

Amazon S3 sur Outposts prend en charge des actions et des filtres de cycle de vie S3 supplémentaires	S3 sur Outposts prend en charge des règles de cycle de vie S3 supplémentaires pour optimiser la gestion de la capacité. Vous pouvez faire expirer des objets lorsqu'ils vieillissent ou sont remplacés par des versions plus récentes. Vous pouvez créer une règle de cycle de vie pour un compartiment entier ou un sous-ensemble d'objets dans un compartiment en filtrant avec des préfixes, des étiquettes d'objets ou la taille des objets. Pour plus d'informations, consultez Création et gestion d'une configuration de cycle de vie.	2 novembre 2022
Prise en charge de la réplication S3 pour les objets SSE-C	Vous pouvez répliquer des objets qui sont créés à l'aide d'un chiffrement côté serveur avec des clés fournies par le client. Pour plus d'informations sur la réplication d'objets chiffrés, consultez Replicating objects created with server-side encryption (SSE-C, SSE-S3, SSE-KMS) [Réplication d'objets créés avec le chiffrement côté serveur (SSE-C, SSE-S3, SSE-KMS)].	24 octobre 2022

Amazon S3 sur Outposts prend en charge les alias de point d'accès	Avec S3 sur Outposts, vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outposts. Chaque fois que vous créez un point d'accès pour un compartiment, S3 sur Outposts génère automatiquement un alias de point d'accès. Vous pouvez utiliser cet alias de point d'accès plutôt qu'un ARN de point d'accès pour toutes les opérations de plan de données. Pour plus d'informations, consultez Utilisation d'un alias de type compartiment pour votre point d'accès S3 on Outposts.	21 octobre 2022
S3 Object Lambda prend en charge les opérations `HeadObject`, `ListObjects` et `ListObjectsV2`	Vous pouvez utiliser du code personnalisé pour modifier les données renvoyées par des requêtes `GET`, `LIST` ou `HEAD` S3 standard afin de filtrer les lignes, de redimensionner les images de manière dynamique, de supprimer des données confidentielles et plus encore. Pour plus d'informations, consultez Transformation d'objets avec S3 Object Lambda.	4 octobre 2022

Amazon S3 sur Outposts prend en charge la gestion des versions S3	Une fois activé, la gestion des versions S3 enregistre plusieurs copies différentes d'un objet dans le même compartiment. Vous pouvez utiliser la gestion des versions S3 pour préserver, récupérer et restaurer chaque version de chaque objet stocké dans votre compartiment Outposts. La gestion des versions S3 vous aide à récupérer en cas d'action involontaire d'un utilisateur et de défaillance applicative. Pour plus d'informations, consultez Gestion de la gestion des versions S3 pour votre compartiment S3 on Outposts.	21 septembre 2022
AWS Backup pour Amazon S3	AWS Backup est un service entièrement géré basé sur des politiques que vous pouvez utiliser pour définir une politique de sauvegarde centralisée afin de protéger vos données Amazon S3. Pour plus d'informations, consultez Utilisation AWS Backup pour Amazon S3.	18 février 2022

Utiliser la réplication par lot S3 pour répliquer des objets existants	Avec la réplication par lot S3, vous pouvez répliquer des objets qui existaient avant la mise en place d'une configuration de réplication. La réplication d'objets existants se fait par l'utilisation d'une tâche d'opérations par lot. La réplication par lot S3 diffère de la réplication en direct qui copie en continu et automatiquement les nouveaux objets d'un compartiment Amazon S3 à l'autre. Pour plus d'informations, consultez Réplication d'objets existants avec la réplication par lot S3.	8 février 2022
Changement de nom de S3 Glacier Flexible Retrieval	La classe de stockage Glacier a été renommée S3 Glacier Flexible Retrieval. Cette modification n'a aucune répercussion sur l'API.	30 novembre 2021

Nouveau paramètre de propriété des objets S3 à désactiver ACLs	Vous pouvez appliquer le paramètre imposé par le propriétaire du compartiment pour la propriété des objets afin de le désactiver ACLs pour votre compartiment et les objets qu'il contient et de vous approprier tous les objets de votre compartiment. Le paramètre appliqué par le propriétaire du compartim ent simplifie la gestion des accès aux données stockées dans Amazon S3. Pour plus d'informations, consultez les sections Contrôle de la propriété des objets et désactivation ACLs de votre compartiment.	30 novembre 2021
Nouvelle classe de stockage S3 Intelligent-Tiering	L'accès S3 Intelligent-Tiering Archive Instant est une classe de stockage supplémentaire sous S3 Intelligent-Tierin g. Pour plus d'informations, consultez Fonctionnement de S3 Intelligent-Tiering.	30 novembre 2021
Nouvelle classe de stockage S3 Glacier Instant Retrieval	Vous pouvez désormais placer des objets dans la classe de stockage S3 Glacier Instant Retrieval. Pour en savoir plus sur cette classe de stockage, utilisez Utilisation des classes de stockage Amazon S3.	30 novembre 2021

AWS Backup pour Amazon S3 Preview	AWS Backup est un service entièrement géré basé sur des politiques que vous pouvez utiliser pour définir une politique de sauvegarde centralisée afin de protéger vos données Amazon S3. Pour plus d'informations, consultez Utilisation AWS Backup pour Amazon S3.	30 novembre 2021
AWS Identity and Access Management Access Analyzer pour Amazon S3	IAM Access Analyzer exécute des vérifications de politique s pour valider votre politique par rapport à la grammaire de politique et aux bonnes pratiques IAM. Pour en savoir plus sur la validatio n des politiques à l'aide d'IAM Access Analyzer, consultez Validation de politique IAM Access Analyzer dans le Guide de l'utilisa teur IAM.	30 novembre 2021
Nouveaux types d'événements	Nouveaux types d'événeme nts ajoutés aux notifications d'événements Amazon S3. Consultez Notifications d'événements Amazon S3.	29 novembre 2021
Activez Amazon EventBridge sur des buckets	Vous pouvez activer EventBrid ge les compartiments Amazon S3 pour envoyer des événements à Amazon EventBridge, voir Utilisation EventBridge.	29 novembre 2021

Nouveaux filtres de cycle de vie S3	Vous pouvez créer des règles de cycle de vie basées sur la taille de l'objet ou spécifier le nombre de versions non courantes de l'objet à conserver. Pour plus d'informations, consultez Examples of S3 Lifecycle configuration (Exemples de configuration du cycle de vie S3).	23 novembre 2021
Publier les métriques d'Amazon S3 Storage Lens sur Amazon CloudWatch	Vous pouvez publier les statistiques d'utilisation et d'activité de S3 Storage Lens sur Amazon CloudWatch afin de créer une vue unifiée de votre santé opérationnelle dans des CloudWatch tableaux de bord. Vous pouvez également utiliser des CloudWatch fonctionnalités, telles que les alarmes et les actions déclenchées, les mathématiques métriques et la détection des anomalies, pour surveiller les métriques S3 Storage Lens et prendre des mesures en conséquence. En outre, ils CloudWatch APIs permettent aux applications, y compris aux fournisseurs tiers, d'accéder à vos métriques S3 Storage Lens. Pour plus d'informations, consultez les métriques Monitor S3 Storage Lens dans CloudWatch.	22 novembre 2021

Points d'accès multi-Régions	Vous pouvez utiliser des points d'accès multi-régions pour créer un point de terminaison global que les applications peuvent utiliser pour traiter les demandes provenant de compartiments Amazon S3 situés dans plusieurs Régions AWS. Vous pouvez utiliser ce point d'accès multi-Régions pour acheminer les données vers un compartiment présentant la latence la plus faible. Pour en savoir plus sur les points d'accès multi-régions et leur utilisation, consultez Point d'accès multi-régions dans Simple Storage Service (Amazon S3).	2 septembre 2021

Amazon S3 sur Outposts ajoute un accès local direct aux applications	Exécutez vos applications en dehors du cloud privé AWS Outposts virtuel (VPC) et accédez à vos données S3 on Outposts. Vous pouvez également accéder aux objets S3 sur Outposts directeme nt depuis votre réseau sur site. Pour en savoir plus sur la configuration des points de terminaison S3 sur Outposts à l'aide des adresses IP clients (CoIP) et l'accès à vos objets en créant une passerelle locale à partir de votre réseau sur site, consultez la section Accès à Amazon S3 sur Outposts à l'aide de points d'accès VPC uniquement.	29 juillet 2021
Alias de points d'accès Amazon S3	Lorsque vous créez un point d'accès, Amazon S3 génère automatiquement un alias que vous pouvez utiliser pour l'accès aux données au lieu d'un nom de compartim ent. Vous pouvez utiliser cet alias de point d'accès plutôt qu'un Amazon Resource Name (ARN) pour toutes les opérations de plan de données de point d'accès. Pour plus d'informations, consultez Utilisation d'un alias de type compartiment pour votre point d'accès.	26 juillet 2021

L'inventaire Amazon S3 et les opérations par lot S3 prennent en charge le statut de la clé de compartiment S3	L'inventaire et les opérations par lot Amazon S3 prennent en charge l'identification et la copie d'objets existants avec des clés de compartiment S3. Les clés de compartiment S3 accélèrent la réduction des coûts de chiffrement côté serveur pour des objets existants. Pour plus d'informations, consultez Inventaire Amazon S3 et Copie d'objet à l'aide d'opérations par lot.	3 juin 2021
Instantané du compte des métriques d'Amazon S3 Storage Lens	L'instantané du compte S3 Storage Lens affiche votre stockage total, le nombre d'objets et la taille moyenne des objets sur la page d'accueil de la console S3 (Buckets (Compartiments) en résumant les métriques de votre tableau de bord par défaut. Pour plus d'informations, consultez Instantané du compte des métriques d'Amazon S3 Storage Lens.	5 mai 2021
Prise en charge accrue des points de terminaison Amazon S3 sur Outposts	S3 sur Outposts prend désormais en charge jusqu'à 100 points de terminaison par Outpost. Pour plus d'informations, consultez Restrictions réseau de S3 on Outposts.	29 avril 2021

Notifications d'événements Amazon S3 on Outposts dans Amazon Events CloudWatch	Vous pouvez utiliser CloudWatch Events pour créer une règle afin de capturer n'importe quel événement de l'API S3 on Outposts et d'être averti par le biais de toutes les cibles prises en charge CloudWatch . Pour plus d'informations, consultez la section Recevoir des notifications d'événements S3 on Outposts à l'aide d' CloudWatch événements.	19 avril 2021
S3 Object Lambda	S3 Object Lambda vous donne la possibilité d'intégrer votre propre code aux requêtes GET Amazon S3 afin de modifier et de traiter les données lorsqu'elles sont renvoyées vers une application. Vous pouvez utiliser du code personnalisé pour modifier les données renvoyées par des requêtes GET S3 standard afin de filtrer les lignes, de redimensionner les images de manière dynamique, de supprimer des données confidentielles et plus encore. Pour plus d'informations, consultez Transformation d'objets.	18 mars 2021

AWS PrivateLink	Avec AWS PrivateLink Amazon S3, vous pouvez vous connecter directement à S3 en utilisant un point de terminaison d'interface dans votre cloud privé virtuel (VPC) au lieu de vous connecter via Internet. Les points de terminaison d'interface sont directement accessibles à partir des applications sur site ou dans une Région AWS différente. Pour plus d'informations, consultez Technologie AWS PrivateLink pour Amazon S3.	2 février 2021
Gérer la capacité d'Amazon S3 on Outposts avec AWS CloudTrail	Les événements de gestion de S3 on Outposts sont disponibles via CloudTrail les journaux. Pour plus d'informations, consultez Gérer la capacité de S3 on Outposts avec CloudTrail	21 décembre 2020

Forte cohérence	Amazon S3 assure une forte read-after-write cohérence pour l'ensemble des objets de votre compartiment S3 PUT et des DELETE requêtes y afférentes Régions AWS. En outre, les opérations de lecture sur Amazon S3 Select, les listes de contrôle d'accès Amazon S3, les balises d'objet Amazon S3 et les métadonnées d'objet (par exemple, l'objet HEAD) sont fortement cohérentes. Pour plus d'informations, consultez Modèle de cohérence de données Amazon S3.	1er décembre 2020

Synchronisation des modifications de réplica Amazon S3	La synchronisation des modifications des répliques Amazon S3 permet de synchroniser les métadonnées des objets ACLs, telles que les balises et les paramètres de verrouillage des objets, entre les objets source et les répliques. Lorsque cette fonctionnalité est activée, Amazon S3 réplique les modifications de métadonnées apportées à l'objet source ou aux copies de réplica. Pour plus d'informations, consultez la Réplication des modifications de métadonnées avec synchronisation des modifications de réplica.	1er décembre 2020

Clés de compartiment Amazon S3	Les clés de compartiment Amazon S3 réduisent le coût du chiffrement côté serveur Amazon S3 à l'aide d' AWS Key Management Service (SSE-KMS). Cette nouvelle clé au niveau du compartiment pour le chiffrement côté serveur peut réduire les coûts des demandes AWS KMS jusqu'à 99 % en diminuant le trafic de demandes d'Amazon S3 vers AWS KMS. Pour plus d'informations, consultez la section Réduire le coût du SSE-KMS à l'aide des clés de compartiment S3.	1er décembre 2020

Amazon S3 Storage Lens	S3 Storage Lens regroupe vos métriques et affiche les informations dans la section Instantané du compte sur la page Compartiments de la console Amazon S3. S3 Storage Lens fournit également un tableau de bord interactif que vous pouvez utiliser pour visualiser les informations et les tendances , signaler les anomalies et recevoir des recommandations pour optimiser les coûts de stockage et appliquer les bonnes pratiques de protectio n des données. Votre tableau de bord dispose d'options d'exploration pour générer et visualiser des informations au niveau de l'organisation, du compte, de la Région AWS, de la classe de stockage, du compartiment, du préfixe ou du groupe Storage Lens. Vous pouvez également envoyer une exportation de métriques quotidienne au format CSV ou Parquet vers un compartim ent S3. Pour plus d'informa tions, consultez Évaluer l'activité et l'utilisation de votre stockage avec S3 Storage Lens.	18 novembre 2020

Suivi des requêtes S3 à l'aide de AWS X-Ray	Amazon S3 s'intègre à X-Ray pour propager le contexte de suivi et vous donner une chaîne de demandes avec des nœuds en amont et en aval. Pour plus d'informations, consultez Suivi des demandes à l'aide de X-Ray.	16 novembre 2020
Métriques de réplication S3	Les métriques de réplication S3 fournissent des métriques détaillées pour les règles de réplication dans votre configuration de réplication. Pour plus d'informations, consultez Métriques de réplication et notifications d'événements Amazon S3.	9 novembre 2020
Accès aux archives S3 Intelligent-Tiering (Hiérarchisation intelligente) et accès à Deep Archive	L'accès aux archives S3 Intelligent-Tiering (Hiérarchisation intelligente) et l'accès à Deep Archive sont des niveaux de stockage supplémentaires dans le cadre de S3 Intelligent-Tiering (Hiérarchisation intelligente). Pour plus d'informations, consultez la Classe de stockage pour optimiser automatiquement les objets fréquemment et rarement consultés.	9 novembre 2020

Réplication des marqueurs de suppression	Avec la réplication des marqueurs de suppression, vous pouvez garantir que les marqueurs de suppressi on sont copiés dans vos compartiments cible pour vos règles de réplication. Pour plus d'informations, consultez Utilisation de la réplication des marqueurs de suppression.	9 novembre 2020
Propriété de l'objet S3	La propriété de l'objet est un paramètre de compartiment S3 que vous pouvez utiliser pour contrôler la propriété des nouveaux objets qui sont téléchargés dans vos compartiments. Pour plus d'informations, consultez Utilisation de la propriété de l'objet S3.	2 octobre 2020

Amazon S3 sur Outposts	Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts ressources et stocker et récupérer facilement des objets sur site pour les applications qui nécessitent un accès aux données locales, un traitement local des données et une résidence des données. Vous pouvez utiliser S3 sur Outposts via l'API AWS Management Console, AWS CLI AWS SDKs, ou REST. Pour plus d'informations, consultez Utilisation d'Amazon S3 sur Outposts.	30 septembre 2020
Condition propriétaire du compartiment	Vous pouvez utiliser la condition de propriétaire du compartiment Amazon S3 pour vous assurer que les compartiments Comptes AWS que vous utilisez dans vos opérations S3 correspondent à vos attentes. Pour plus d'informations, consultez Condition propriétaire du compartiment.	11 septembre 2020

Prise en charge des opérations par lot S3 pour la rétention du verrouillage d'objet	Vous pouvez désormais utiliser les opérations par lot avec le verrouillage d'objet S3 pour appliquer des paramètres de conservation à de nombreux objets Simple Storage Service (Amazon S3) à la fois. Pour plus d'informations, consultez Définition des dates de rétention du verrouillage d'objets S3 à l'aide des opérations par lot S3.	4 mai 2020
Prise en charge des opérations par lot S3 pour la conservation légale du verrouillage d'objet	Vous pouvez désormais utiliser les opérations par lot avec le verrouillage d'objet S3 pour ajouter une conservation légale à de nombreux objets Amazon S3 à la fois. Pour plus d'informations, consultez Utilisation des opérations par lot S3 pour définir la conservation légale du verrouillage d'objet S3.	4 mai 2020
Balises de tâche pour les opérations par lot S3	Vous pouvez ajouter des balises à vos tâches d'opérations par lot S3 pour contrôler et étiqueter ces tâches. Pour plus d'informations, consultez Balises pour les tâches d'opérations par lot S3.	16 mars 2020

Points d'accès Amazon S3	Les points d'accès Amazon S3 simplifient la gestion de l'accès aux données à grande échelle pour les jeux de données partagés dans S3. Les points d'accès sont des points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet S3. Pour plus d'informations, consultez la rubrique Gestion de l'accès aux données à l'aide des points d'accès Amazon S3.	2 décembre 2019
Analyseur d'accès pour Amazon S3	Access Analyzer pour Amazon S3 vous avertit de la présence de compartiments S3 configurés pour autoriser l'accès à toute personne sur Internet ou autre Comptes AWS, y compris à des comptes extérieurs à votre organisation. Pour plus d'informations, consultez Utilisation de l'analyseur d'accès pour Amazon S3.	2 décembre 2019

Contrôle du délai de réplication S3 (S3 RTC)	Le contrôle du délai de réplication S3 (S3 RTC) réplique la plupart des objets téléchargés sur Amazon S3 en quelques secondes, et 99,99 % de ces objets dans les 15 minutes. Pour plus d'informations, consultez Réplication d'objets à l'aide du contrôle du temps de réplication S3 (S3 RTC).	20 novembre 2019
Réplication dans une même Région	Vous pouvez utiliser la réplication dans une même région (SRR) pour copier des objets entre compartiments Amazon S3 d'une même Région AWS. Pour plus d'informations sur la réplication entre Régions et la réplication dans une même région, consultez Réplication.	18 septembre 2019
Prise en charge de la réplication entre Régions pour le verrouillage d'objet S3	La réplication entre Régions prend désormais en charge le verrouillage d'objet. Pour plus d'informations, consultez Qu'est-ce qu'Amazon S3 réplique ?.	28 mai 2019

Opérations par lot S3	À l'aide des opérations par lot S3, vous pouvez effectuer des opérations par lot à grande échelle sur des objets Amazon S3. Les opérations par lot S3 peuvent exécuter une seule opération sur les listes d'objets que vous spécifiez. Un même travail peut effectuer l'opération spécifiée sur des milliards d'objets contenant des exaoctets de données. Pour plus d'informations, consultez la section Exécution des Opérations par lot S3.	30 avril 2019
Région Asie-Pacifique (Hong Kong)	Amazon S3 est désormais disponible dans la Région Asie-Pacifique (Hong Kong). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	24 avril 2019
Nouveau champ ajouté aux journaux d'accès au serveur	Amazon S3 a ajouté le nouveau champ suivant aux journaux d'accès au serveur : version de protocole TLS (Transport Layer Security) . Pour plus d'informations, consultez Format des journaux d'accès au serveur.	28 mars 2019

Nouvelle classe de stockage d'archive	Amazon S3 propose désormais une nouvelle classe de stockage d'archive , S3 Glacier Deep Archive (`DEEP_ARCHIVE`), pour le stockage d'objets rarement consultés. Pour plus d'informations, consultez Classes de stockage.	27 mars 2019
Nouveaux champs ajoutés aux journaux d'accès au serveur	Amazon S3 a ajouté les nouveaux champs suivants aux journaux d'accès au serveur : Host Id, Signature Version, Cipher Suite, Authentication Type et Host Header. Pour plus d'informations, consultez Format des journaux d'accès au serveur.	5 mars 2019
Prise en charge des fichiers Amazon S3 Inventory au format Parquet	Simple Storage Service (Amazon S3) prend désormais en charge le format Apache Parquet (Parquet) en plus du format Apache ORC (Optimized Row Columnar) et du format de fichier CSV (valeurs séparées par une virgule) pour les fichiers de sortie d'inventaire. Pour plus d'informations, consultez Inventaire.	4 décembre 2018

Verrouillage des objets S3	Amazon S3 prend désormais en charge la fonctionnalité de verrouillage d'objets qui fournit les protections Write Once Read Many (WORM) pour les objets Amazon S3. Pour plus d'informations, consultez Verrouillage des objets.	26 novembre 2018
Mise à niveau de la vitesse de restauration	À l'aide de la mise à niveau de la vitesse de restauration Amazon S3, vous pouvez accélérer la vitesse d'une restauration depuis la classe de stockage S3 Glacier Flexible Retrieval pendant que la restauration est en cours. Pour plus d'informations, consultez Restauration des objets archivés.	26 novembre 2018
Notifications d'événement de restauration	Les notifications d'événement Amazon S3 prennent désormais en charge le lancement et l'arrêt des événements lors de la restauration des objets depuis la classe de stockage S3 Glacier Flexible Retrieval. Pour plus d'informations, consultez Notifications d'événement.	26 novembre 2018

PUT directement sur la classe de stockage S3 Glacier Flexible Retrieval	L'opération PUT Amazon S3 prend désormais en charge la spécification S3 Glacier Flexible Retrieval comme classe de stockage lorsque vous créez des objets. Avant, vous deviez transférer les objets vers la classe de stockage S3 Glacier Flexible Retrieval à partir d'une autre classe de stockage Amazon S3. De même, lorsque vous utilisez la réplication entre Régions S3, vous pouvez désormais spécifier S3 Glacier Flexible Retrieval comme classe de stockage pour les objets répliqués . Pour en savoir plus sur la classe de stockage S3 Glacier Flexible Retrieval , consultez Classes de stockage. Pour en savoir plus sur la spécification de la classe de stockage pour les objets répliqués, consultez Présentation de la configuration de réplication. Pour plus d'informations sur la modification de la commande directe PUT sur l'API REST S3 Glacier Flexible Retrieval , consultez Historique du document :	26 novembre 2018

	PUT directement sur S3 Glacier Flexible Retrieval.	
Nouvelle classe de stockage	Amazon S3 propose une nouvelle classe de stockage nommée S3 Intelligent-Tiering (`INTELLIGENT_TIERING`) conçue pour les données de longue durée avec des modèles d'accès variables ou inconnus. Pour plus d'informations, consultez Classes de stockage.	26 novembre 2018
Blocage de l'accès public Amazon S3	Amazon S3 inclut désormais la possibilité de bloquer l'accès public aux compartiments et aux objets par compartiment ou à l'échelle d'un compte. Pour plus d'informations, consultez Utilisation de la fonctionnalité de blocage de l'accès public Amazon S3.	15 novembre 2018

Filtrage des améliorations dans les règles de la réplication entre Régions (CRR)	Dans une configuration de règle CRR, vous pouvez spécifier un filtre d'objet pour choisir un sous-ensemble d'objets auquel s'applique la règle. Précédemment, vous ne pouviez filtrer que sur un préfixe de clé d'objet. Dans cette version, vous pouvez filtrer sur un préfixe de clé d'objet, une ou plusieurs balises d'objet, ou les deux. Pour plus d'informations, consultez la Configuration CRR : présentation de la configuration de réplication.	19 septembre 2018
Nouvelles fonctions d'Amazon S3 Select	Amazon S3 Select prend désormais en charge les entrées Apache Parquet, les requêtes sur des objets JSON imbriqués et deux nouvelles métriques CloudWatch de surveillance Amazon (`SelectScannedBytes` et `SelectReturnedBytes`).	5 septembre 2018
Mises à jour disponibles sur RSS	Vous pouvez à présent vous abonner à un flux RSS pour recevoir les notifications des mises à jour du Guide d'utilisateur Amazon S3.	19 juin 2018

Mises à jour antérieures

Le tableau ci-après décrit les modifications importantes apportées dans chaque version du Guide de l'utilisateur Amazon S3 avant le 19 juin 2018.

Modification	Description	Date
Mise à jour d'exemples de code	Exemples de code mis à jour : • C# - Mise à jour de l'ensemble des exemples afin d'utiliser le modèle asynchrone basé sur tâche. Pour plus d'informations, consultez Amazon Web Services Asynchronous APIs pour .NET dans le Guide du AWS SDK pour .NET développeur. Les exemples de code fournis sont désormais compatibles avec la version 3 du kit AWS SDK pour .NET. • Java - Mise à jour de l'ensemble des exemples afin d'utiliser le modèle de générateur client. Pour plus d'informations sur le modèle de générateur client, consultez Création de clients de service. • PHP - Mise à jour de l'ensemble des exemples afin d'utiliser le kit AWS SDK pour PHP 3.0. Pour plus d'informations sur la AWS SDK pour PHP version 3.0, consultez AWS SDK pour PHP. • Ruby : exemple de code mis à jour afin que les exemples fonctionnent avec la AWS SDK pour Ruby version 3.	30 avril 2018
Amazon S3 indique désormais les classes de récupération et de `ONEZONE_IA` stockage flexibles de S3 Glacier dans les métriques de stockage	Outre les octets effectifs, ces métriques de stockage comprennent les octets de supplément par objet pour les classes de stockage applicables (`ONEZONE_IA` , `STANDARD_IA` et S3 Glacier Flexible Retrieval) : •	30 avril 2018

Modification	Description	Date

d'Amazon CloudWatch Logs	Pour les objets de classe de stockage `ONEZONE_IA` et `STANDARD_IA` , Simple Storage Service (Amazon S3) rapporte les objets de taille inférieure à 128 Ko comme ayant une taille de 128 Ko. Pour plus d'informations, consultez Bien comprendre et gérer les classes de stockage Amazon S3.
	• Pour les objets de classe de stockage S3 Glacier Flexible Retrieval, les métriques de stockage rapportent les suppléments suivants :
	  • Un supplément de 32 Ko par objet, facturé au tarif de la classe de stockage S3 Glacier Flexible Retrieval
	  • Un supplément de 8 Ko par objet, facturé au tarif de la classe de stockage `STANDARD`
	  Pour plus d'informations, consultez Transition des objets à l'aide du cycle de vie Amazon S3.
	
	Pour plus d'informations sur les métriques de stockage, consultez Surveillance des métriques avec Amazon CloudWatch.	

Nouvelle classe de stockage	Amazon S3 propose désormais une nouvelle classe de stockage, `STANDARD_IA` (où « IA » signifie « infrequent access », ou accès peu fréquent) pour le stockage d'objets. Cette classe de stockage est optimisée pour les données à longue durée de vie et moins fréquemment consultées. Pour plus d'informations, consultez Bien comprendre et gérer les classes de stockage Amazon S3.	4 avril 2018

Modification	Description	Date
Amazon S3 Select	Amazon S3 prend désormais en charge la récupération de contenu d'objet basée sur une expression SQL. Pour de plus amples informations, veuillez consulter Interrogation des données sur place avec Amazon S3 Select.	4 avril 2018
Région Asie-Pacifique (Osaka-Local)	Amazon S3 est maintenant disponible dans la Région Asie-Pacifique (Osaka-Local). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS. **Important** Vous pouvez utiliser la Région Asie-Pacifique (Osaka-Local) uniquement en conjonction avec la Région Asie-Pacifique (Tokyo). Pour demander l'accès à la Région Asie-Pacifique (Osaka-Local), veuillez contacter votre représentant commercial.	12 février 2018
Horodatage de création d'Amazon S3 Inventory	Amazon S3 Inventory comprend désormais un horodatage de la date et de l'heure du début de la création du rapport Amazon S3 Inventory. Vous pouvez utiliser l'horodatage pour déterminer les modifications dans votre stockage Amazon S3 à partir de la date de début ou lorsque le rapport d'inventaire a été généré.	16 janvier 2018
Région Europe (Paris)	Amazon S3 est désormais disponible dans la Région Europe (Paris). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	18 décembre 2017
Région Chine (Ningxia)	Amazon S3 est désormais disponible dans la Région Chine (Ningxia). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	29 novembre 2017

Modification	Description	Date
Prise en charge des fichiers Amazon S3 Inventory au format ORC	Amazon S3 prend désormais en charge le format Apache ORC (Optimized Row Columnar) en plus du format de fichier CSV (valeurs séparées par une virgule) pour les fichiers de sortie d'inventaire. Vous pouvez également interroger l'inventaire Amazon S3 en utilisant SQL standard à l'aide d'Amazon Athena, Amazon Redshift Spectrum et d'autres outils tels que Presto, Apache Hive et Apache Spark. Pour plus d'informations, consultez Catalogage et analyse de vos données avec l'inventaire S3.	17 novembre 2017
Chiffrement par défaut pour les compartiments S3	Le chiffrement par défaut d'Amazon S3 permet de définir le comportement de chiffrement par défaut pour un compartiment S3. Vous pouvez définir le chiffrement par défaut sur un compartiment afin que tous les objets soient chiffrés lorsqu'ils sont stockés dans le compartiment. Les objets sont chiffrés à l'aide du chiffrement côté serveur avec des clés gérées Amazon S3 (SSE-S3) ou des clés AWS gérées (SSE-KMS). Pour de plus amples informations, veuillez consulter Définition du comportement de chiffrement côté serveur par défaut pour les compartiments Amazon S3.	06 novembre 2017
Statut de chiffrement dans Amazon S3 Inventory	Amazon S3 prend désormais en charge l'inclusion du statut de chiffrement dans Amazon S3 Inventory afin que vous puissiez voir comment vos objets sont chiffrés au repos pour des audits de conformité ou à d'autres fins. Vous pouvez également configurer le chiffrement d'Amazon S3 Inventory avec le chiffrement côté serveur (SSE) ou SSE-KMS afin que tous les fichiers d'inventaire soient chiffrés en conséquence. Pour plus d'informations, consultez Catalogage et analyse de vos données avec l'inventaire S3.	06 novembre 2017

Modification	Description	Date
Améliorations de la réplication entre Régions (CRR)	La réplication entre Régions prend désormais en charge les aspects suivants : • Dans un scénario à plusieurs comptes, vous pouvez ajouter une configuration CRR pour remplacer le propriétaire des réplicas par le Compte AWS qui détient le compartiment de destination. Pour de plus amples informations, veuillez consulter Modification du propriétaire d'un réplica. • Par défaut, Amazon S3 ne réplique pas les objets de votre compartiment source créés à l'aide du chiffrement côté serveur à l'aide de clés stockées AWS KMS dans votre configuration CRR, vous pouvez désormais demander à Amazon S3 de répliquer ces objets. Pour de plus amples informations, veuillez consulter Réplication d'objets chiffrés (SSE-S3, SSE-KMS, DSSE-KMS, SSE-C).	06 novembre 2017
Région Europe (Londres)	Amazon S3 est désormais disponible dans la Région Europe (Londres). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	13 décembre 2016
Région Canada (Centre)	Amazon S3 est désormais disponible dans la Région Canada (Centre). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	8 décembre 2016

Modification	Description	Date
Balisage des objets	Amazon S3 prend désormais en charge le balisage des objets. Le balisage des objets vous permet de classer le stockage par catégorie. Les préfixes des noms de clés d'objet vous permettent également de classer le stockage par catégorie ; le balisage des objets y ajoute une autre dimension. Il existe des avantages supplémentaires offerts par le balisage. Il s'agit des licences suivantes : • Les balises d'objets permettent un contrôle d'accès précis des autorisations (par exemple, vous pouvez octroyer des autorisations aux utilisateurs IAM pour lire uniquement des objets avec des balises spécifiques). • Contrôle précis en spécifiant la configuration du cycle de vie. Vous pouvez spécifier des balises pour sélectionner un sous-ensemble d'objets auxquels la règle de cycle de vie s'applique. • Si vous avez configuré la réplication entre Régions (CRR), Amazon S3 peut répliquer les balises. Vous devez octroyer les autorisations nécessaires au rôle IAM assumé par Amazon S3 pour répliquer des objets en votre nom. • Vous pouvez également personnaliser CloudWatch les mesures et les CloudTrail événements pour afficher les informations par le biais de filtres de balises spécifiques. Pour de plus amples informations, veuillez consulter Catégorisation de vos objets à l'aide de balises.	29 novembre 2016

Modification	Description	Date
Le cycle de vie Amazon S3 prend désormais en charge les filtres basés sur les balises.	Amazon S3 prend désormais en charge le filtrage basé sur des balises dans la configuration du cycle de vie. Vous avez la possibilité de spécifier les règles de cycle de vie dans lesquelles vous pouvez indiquer un préfixe de clé, une ou plusieurs balises d'objets, ou une combinaison des deux pour sélectionner un sous-ensemble d'objets auquel la règle de cycle de vie s'applique. Pour plus d'informations, consultez Gestion du cycle de vie des objets.	29 novembre 2016
CloudWatch mesures de demande pour les buckets	Amazon S3 prend désormais en charge CloudWatch les métriques pour les demandes effectuées sur des buckets. Lorsque vous activez ces métriques pour un compartiment, les métriques fournissent des résultats toutes les minutes. Vous pouvez également configurer les objets d'un compartiment qui signaleront ces métriques de demandes. Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch.	29 novembre 2016
Inventaire Amazon S3	Amazon S3 prend désormais en charge l'inventaire de stockage. Amazon S3 Inventory fournit une sortie de fichiers plats de vos objets et leurs métadonnées correspondantes sur une base quotidienne ou hebdomadaire pour un compartiment S3 ou un préfixe partagé (c'est-à-dire, les objets qui ont des noms qui commencent par une chaîne commune). Pour plus d'informations, consultez Catalogage et analyse de vos données avec l'inventaire S3.	29 novembre 2016

Modification	Description	Date
Analyses Amazon S3 – Analyse de classe de stockage	La nouvelle fonction d'analyse de classe de stockage Amazon S3 observe les modèles d'accès aux données afin de vous aider à déterminer le moment approprié pour passer du mode `STANDARD` au mode `STANDARD_IA` (« IA » correspondant à « infrequent access », soit accès peu fréquents). Une fois que l'analyse de classe de stockage a observé les modèles d'accès peu fréquents d'un ensemble filtré de données sur une période donnée, vous pouvez utiliser les résultats d'analyse pour vous aider à améliorer vos configurations de cycle de vie. Cette fonction comprend également une analyse détaillée quotidienne de votre utilisation du stockage au niveau du compartiment, du préfixe ou de la balise que vous pouvez exporter vers un compartiment S3.	29 novembre 2016
Nouvelles récupérations de données rapides et en bloc lors de la restauration d'objets archivés de S3 Glacier.	Amazon S3 prend désormais en charge les récupérations de données rapides et en bloc en plus des récupérations standard lors de la restauration d'objets archivés sur S3 Glacier. Pour plus d'informations, consultez Restauration d'un objet archivé.	21 novembre 2016
CloudTrail journalisation des objets	CloudTrail prend en charge la journalisation des opérations d'API au niveau des objets Amazon S3`GetObject`, telles que`PutObject`, et`DeleteObject`. Vous pouvez configurer votre sélecteur d'événements de sorte qu'il enregistre les opérations API au niveau de l'objet. Pour plus d'informations, consultez Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail.	21 novembre 2016
Région USA Est (Ohio)	Amazon S3 est désormais disponible dans la Région USA Est (Ohio). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	17 octobre 2016

Modification	Description	Date
IPv6 prise en charge d'Amazon S3 Transfer Acceleration	Amazon S3 prend désormais en charge le protocole Internet version 6 (IPv6) pour Amazon S3 Transfer Acceleration. Vous pouvez vous connecter à Amazon S3 IPv6 en utilisant le nouveau point de terminaison Dual-Stack for Transfer Acceleration. Pour de plus amples informations, veuillez consulter Mise en route d'Amazon S3 Transfer Acceleration.	6 octobre 2016
IPv6 soutien	Amazon S3 prend désormais en charge la version 6 du protocole Internet (IPv6). Vous pouvez accéder à Amazon S3 via des points IPv6 de terminaison à double pile. Pour plus d'informations, consultez la section Faire des demandes à Amazon S3 IPv6 dans le manuel de référence des API Amazon S3.	11 août 2016
Région Asie-Pacifique (Mumbai)	Amazon S3 est désormais disponible dans la Région Asie-Pacifique (Mumbai). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	27 juin 2016
Amazon S3 Transfer Acc ion	Amazon S3 Transfer Acceleration permet un transfert rapide, facile et sécurisé de fichiers sur des longues distances entre votre client et un compartiment S3. Transfer Acceleration tire parti des emplacements périphéri ques distribués par Amazon CloudFront dans le monde entier. Pour de plus amples informations, veuillez consulter Configuration de transferts de fichiers rapides et sécurisés à l'aide d'Amazon S3 Transfer Acceleration.	19 avril 2016

Modification	Description	Date
Prise en charge du cycle de vie pour supprimer les marqueurs de suppression des objets expirés	L'action `Expiration` de configuration de cycle de vie vous permet d'indiquer à Amazon S3 de supprimer les marqueurs de suppression des objets expirés dans un compartiment avec gestion des versions. Pour plus d'informations, consultez Éléments pour décrire les actions du cycle de vie.	16 mars 2016

Modification	Description	Date
La configuration de cycle de vie du compartiment prend désormais en charge l'arrêt des chargements partitionnés inachevés	La configuration de cycle de vie du compartiment prend désormais en charge l'action `AbortIncompleteMultipartUpload` permettant de demander à Amazon S3 d'arrêter les chargements partitionnés qui ne sont pas terminés au bout d'un certain nombre de jours après leur lancement. Si un chargement partitionné est susceptible de faire l'objet d'un arrêt, Amazon S3 supprime les parties téléchargées et arrête le chargement partitionné. Pour obtenir des informations conceptuelles, consultez les rubriques suivantes dans le Guide de l'utilisateur Amazon S3 : • Interruption d'un chargement partitionné • Éléments pour décrire les actions du cycle de vie Les opérations API suivantes ont été mises à jour afin de prendre en charge cette nouvelle action : • PutBucketLifecycle – La configuration XML permet désormais de spécifier l'action `AbortIncompleteMultipartUpload` dans une règle de configuration de cycle de vie. • ListParts et InitiateMultipartUpload – Ces deux opérations d'API renvoient désormais deux en-têtes de réponse supplémentaires (`x-amz-abort-date` et `x-amz-abort-rule-id`) si le compartiment dispose d'une règle de cycle de vie spécifiant l'action `AbortIncompleteMultipartUpload`. Ces en-têtes dans la réponse indiquent quand le chargement partitionné peut faire l'objet d'une opération d'arrêt et quelle règle de cycle de vie s'applique.	16 mars 2016

Modification	Description	Date
Région Asie-Pacifique (Séoul)	Amazon S3 est désormais disponible dans la Région Asie-Pacifique (Séoul). Pour plus d'informations sur les régions et les points de terminaison Amazon S3, consultez Régions et points de terminaison dans la Références générales AWS.	6 janvier 2016
Nouvelle clé de condition et modification du chargement partitionné	Les politiques IAM prennent désormais en charge une clé de condition `s3:x-amz-storage-class` Amazon S3. Pour plus d'informations, consultez Exemples de politiques de compartiment utilisant des clés de condition. Il n'est plus nécessaire que vous soyez à l'origine du chargement partitionné pour charger des parties et terminer le chargement. Pour plus d'informations, consultez API de chargement partitionné et autorisations.	14 décembre 2015
Région USA Standard renommée	Modification de l'intitulé de la Région « USA Standard » par « USA Est (Virginie du Nord) ». Seul le nom a été mis à jour, la fonctionnalité demeure inchangée.	11 décembre 2015

Modification	Description	Date
Nouvelle classe de stockage	Amazon S3 propose désormais une nouvelle classe de stockage, STANDARD_IA (où « IA » signifie « infrequent access », ou accès peu fréquent) pour le stockage d'objets. Cette classe de stockage est optimisée pour les données à longue durée de vie et moins fréquemment consultées. Pour plus d'informations, consultez Bien comprendre et gérer les classes de stockage Amazon S3. Les mises à jour apportées à la fonctionnalité de configuration de cycle de vie permettent désormais la transition d'objets vers la classe de stockage STANDARD_IA. Pour plus d'informations, consultez Gestion du cycle de vie des objets. Jusqu'ici, la fonctionnalité de réplication entre Régions utilisait la classe de stockage de l'objet source pour créer un réplica de l'objet. Désormais, lorsque vous configurez la réplication entre Régions, vous pouvez spécifier une classe de stockage pour le réplica de l'objet créé dans le compartiment de destination. Pour plus d'informations, consultez Réplication d'objets au sein des régions et entre elles.	16 septembre 2015
AWS CloudTrail intégration	La nouvelle AWS CloudTrail intégration vous permet d'enregistrer l'activité de l'API Amazon S3 dans votre compartiment S3. Vous pouvez l'utiliser CloudTrail pour suivre les créations ou les suppressions de compartiments S3, les modifications du contrôle d'accès ou les modifications de configuration du cycle de vie. Pour de plus amples informations, veuillez consulter Journalisation des appels d'API Amazon S3 à l'aide de AWS CloudTrail.	1er septembre 201

Modification	Description	Date
Augmentation de limite de compartiment	Amazon S3 prend désormais en charge les augmentations de limite de compartiment. Par défaut, les clients peuvent créer jusqu'à 100 compartiments dans leur Compte AWS Les clients ayant besoin de compartiments supplémentaires peuvent envoyer une demande afin d'augmenter la limite du service. Pour obtenir des informations sur la manière d'augmenter votre limite de compartiment, consultez Quotas de Service AWS dans la Référence générale d'AWS . Pour plus d'informations, consultez À l'aide du AWS SDKs et Quotas, limites et restrictions relatifs aux compartiments à usage général.	4 août 2015
Mise à jour du modèle de cohérence (consistency)	Amazon S3 prend désormais en charge read-after-write la cohérence pour les nouveaux objets ajoutés à Amazon S3 dans la région de l'est des États-Unis (Virginie du Nord). Avant cette mise à jour, toutes les régions, à l'exception de la région USA Est (Virginie du Nord), read-after-write prenaient en charge la cohérence pour les nouveaux objets chargés sur Amazon S3. Grâce à cette amélioration, Amazon S3 assure désormais read-after-write la cohérence dans toutes les régions pour les nouveaux objets ajoutés à Amazon S3. Read-after-writela cohérence vous permet de récupérer des objets immédiatement après leur création dans Amazon S3. Pour de plus amples informations, veuillez consulter Régions.	4 août 2015
Notifications d'événements	La fonctionnalité de notification d'événement d'Amazon S3 a été mise à jour, ce qui vous permet désormais d'envoyer des notifications lorsque des objets sont supprimés et de filtrer les objets par nom d'objet dont le préfixe et le suffixe correspondent. Pour plus d'informations, consultez Notifications d'événements Amazon S3.	28 juillet 2015

Modification	Description	Date
CloudWatch Intégration avec Amazon	La nouvelle CloudWatch intégration d'Amazon vous permet de surveiller et de définir des alarmes relatives à votre utilisation d'Amazon S3 grâce à CloudWatch des métriques pour Amazon S3. Les indicateurs pris en charge sont la quantité totale d'octets pour le stockage standard, la quantité totale d'octets pour le stockage RRS et le nombre total d'objets pour un compartiment S3 donné. Pour plus d'informations, consultez Surveillance des métriques avec Amazon CloudWatch.	28 juillet 2015
Prise en charge de la suppression et du vidage des compartiments non vides	Amazon S3 vous permet désormais de supprimer et de vider les compartiments non vides. Pour plus d'informations, consultez Vidange d'un seau à usage général.	16 juillet 2015
Politiques de compartiment pour les points de terminaison d'un VPC Amazon	Amazon S3 a ajouté la prise en charge des stratégies de compartiment pour les points de terminaison de VPC. Vous pouvez utiliser les politiques de compartiment S3 pour contrôler l'accès aux compartiments à partir de points de terminaison VPC spécifiques ou spécifiques. VPCs Les points de terminaison d'un VPC sont faciles à configurer et assurent une connectivité fiable à Amazon S3 sans qu'une passerelle Internet ou une instance NAT soit nécessaire. Pour plus d'informations, consultez Contrôle de l'accès à partir des points de terminaison d'un VPC avec des stratégies de compartiment.	29 avril 2015
Notifications d'événements	Les notifications d'événements Amazon S3 ont été mises à jour pour permettre le passage à des autorisations basées sur les ressources pour AWS Lambda les fonctions. Pour de plus amples informations, veuillez consulter Notifications d'événements Amazon S3.	9 avril 2015

Modification	Description	Date
Réplication entre Régions	Amazon S3 prend désormais en charge la réplication entre Régions. La réplication entre régions est la copie automatiq ue et asynchrone d'objets dans différents compartiments. Régions AWS Pour de plus amples informations, veuillez consulter Réplication d'objets au sein des régions et entre elles.	24 mars 2015
Notifications d'événements	Amazon S3 prend désormais en charge de nouveaux types d'événements et de nouvelles destinations pour la configuration des notifications de compartiment. Avant cette version, Amazon S3 ne prenait en charge que le type d'ReducedRedundancyLostObjectévénement s3 : et une rubrique Amazon SNS comme destination. Pour plus d'informations sur les nouveaux types d'événements, consultez Notifications d'événements Amazon S3.	13 novembre 2014
Chiffrement côté serveur à l'aide des clés de chiffrement fournies par le client	Chiffrement côté serveur avec clés AWS Key Management Service (AWS KMS) (SSE-KMS) Amazon S3 prend désormais en charge le chiffrement côté serveur à l'aide de. AWS KMS Cette fonctionnalité vous permet de gérer la clé d'enveloppe et Amazon S3 appelle A WS KMS pour accéder à la clé d'enveloppe dans les limites des autorisations que vous avez définies. AWS KMS Pour plus d'informations sur le chiffrement côté serveur avec AWS KMS, voir Protection des données à l'aide du chiffrement côté serveur avec. AWS Key Management Service	12 novembre 2014
Région Europe (Francfort)	Amazon S3 est maintenant disponible dans la Région Europe (Francfort).	23 octobre 2014

Modification	Description	Date
Chiffrement côté serveur à l'aide des clés de chiffrement fournies par le client	Amazon S3 prend désormais en charge le chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C). Le chiffrement côté serveur vous permet de demander à Amazon S3 de chiffrer vos données au repos. Lorsque vous utilisez SSE-C, Amazon S3 chiffre vos objets grâce aux clés de chiffrement personnalisées que vous fournissez. Étant donné qu'Amazon S3 effectue le chiffrement pour vous, vous bénéficiez de l'avantage d'utiliser vos propres clés de chiffrement sans encourir le coût lié à l'écriture ou l'exécution de votre propre code de chiffrement. Pour plus d'informations sur SSE-C, consultez Chiffrement côté serveur (à l'aide des clés de chiffrement fournies par le client).	12 juin 2014
Prise en charge du cycle de vie pour la gestion des versions	Avant cette publication, la configuration de cycle de vie était prise en charge uniquement sur les compartiments non versionnés. Vous pouvez désormais configurer le cycle de vie aussi bien sur les compartiments non versionné s que les compartiments pour lesquels la gestion des versions d'objet est activée. Pour plus d'informations, consultez Gestion du cycle de vie des objets.	20 mai 2014
Révision des rubriques consacrées au contrôle d'accès	Révision de la documentation consacrée au contrôle d'accès Amazon S3. Pour de plus amples informations, veuillez consulter Gestion des identités et des accès pour Amazon S3.	15 avril 2014
Révision de la rubrique consacrée à la journalisation des accès au serveur	Révision de la documentation consacrée à la journalisation des accès au serveur. Pour plus d'informations, consultez Enregistrement de demandes avec journalisation des accès au serveur.	26 novembre 2013

Modification	Description	Date
Exemples SDK pour .NET mis à jour dans la version 2.0	Les exemples SDK pour .NET fournis dans ce guide sont désormais compatibles avec la version 2.0.	26 novembre 2013
Obsolescence de la prise en charge SOAP via HTTP	La prise en charge de SOAP via HTTP est obsolète, mais continue d'être disponible sur HTTP. Les nouvelles fonctionnalités Amazon S3 ne sont pas prises en charge pour SOAP. Nous vous recommandons d'utiliser l'API REST ou le AWS SDKs.	20 septembre 201
Prise en charge des variables dans la politique IAM	Le langage de la politique IAM prend désormais en charge des variables. Lorsqu'une stratégie est évaluée, toutes les variables de stratégie sont remplacées par des valeurs issues d'informations basées sur le contexte provenant de la session de l'utilisateur authentifié. Vous pouvez utiliser des variables de stratégie pour définir des stratégie s à usage général sans dresser de manière explicite la liste des éléments composant cette stratégie. Pour plus d'informations sur les variables de politique, consultez Présentation des variables de la politique IAM dans le Guide de l'utilisateur IAM. Pour obtenir des exemples de variables de stratégies dans Amazon S3, consultez Exemples de politiques basées sur l'identité pour Amazon S3.	3 avril 2013
Prise en charge via la console du paiement par le demandeur	Vous pouvez désormais configurer votre compartiment pour le Paiement par le demandeur via la console Amazon S3. Pour plus d'informations, consultez Utilisation des compartiments à usage général de Requester Pays pour le stockage, les transferts et l'utilisation.	31 décembre 2012

Modification	Description	Date
Prise en charge du domaine racine pour l'hébergement de site Web	Amazon S3 prend désormais en charge l'hébergement de sites web dans le domaine racine. Les internautes de votre site Internet peuvent ainsi accéder à votre site à partir de leur navigateur sans devoir saisir www dans l'adresse Web (par exemple, ils peuvent utiliser example.com au lieu de www.example.com). De nombreux clients hébergent déjà des sites web statiques sur Amazon S3, accessibles à partir d'un sous-domaine www (par exemple, www.example.com). Jusqu'ici, pour permettre l'accès au domaine racine, vous deviez exécuter votre propre serveur web afin qu'il fasse office de proxy pour les demandes du domaine racine depuis les navigateurs jusqu'à votre site web Amazon S3. L'exécution d'un serveur Web vers des demandes proxy entraînait des frais supplémentaires, alourdissait la charge opérationnelle et introduisait un point de défaillance potentiel. Vous pouvez désormais profiter de la grande disponibilité et durabilité d'Amazon S3 aussi bien pour les adresses de type www que les adresses de domaine racine. Pour plus d'informations, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.	27 décembre 2012
Révision de la console	Nous avons mis à jour la console Amazon S3. Les rubriques de la documentation se rapportant à la console ont donc été révisées en conséquence.	14 décembre 2012

Modification	Description	Date
Prise en charge de l'archivage des données dans S3 Glacier	Amazon S3 prend désormais en charge une option de stockage qui vous permet d'exploiter le service de stockage économique de S3 Glacier pour l'archivage des données. Pour archiver des objets, vous devez définir des règles d'archivage identifiant des objets ainsi qu'un calendrier pour indiquer quand Amazon S3 doit archiver ces objets sur S3 Glacier. Vous pouvez facilement définir les règles d'un compartiment à l'aide de la console Amazon S3 ou par programmation à l'aide de l'API Amazon S3 ou. AWS SDKs Pour de plus amples informations, veuillez consulter Gestion du cycle de vie des objets.	13 novembre 2012
Prise en charge des redirections de page de site Web	Pour un compartiment configuré comme un site web, Amazon S3 prend désormais en charge la redirection d'une demande pour un objet vers un autre objet dans le même compartiment ou vers une URL externe. Pour plus d'informations, consultez (Facultatif) Configuration de la redirection de pages web. Pour obtenir des informations sur l'hébergement de sites Web, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.	4 octobre 2012

Modification	Description	Date
Prise en charge du partage des ressources cross-origin (CORS)	Amazon S3 prend désormais en charge le partage des ressources cross-origin (CORS). Le mécanisme CORS permet aux applications Web clientes chargées dans un domaine donné d'interagir avec les ressources d'un autre domaine ou d'y accéder. Avec le support CORS dans Amazon S3, vous pouvez créer des applications web clientes denses riches sur Amazon S3 et de manière sélective permettre un accès cross-domaine à vos ressources Amazon S3. Pour plus d'informations, consultez Utilisation du partage des ressources entre origines multiples (CORS).	31 août 2012
Prise en charge des balises de répartition des coûts	Amazon S3 prend désormais en charge le balisage de répartition des coûts qui permet d'étiqueter les compartiments S3 et ainsi de faciliter le suivi de leurs coûts en fonction des projets ou d'autres critères. Pour plus d'informations sur le balisage des compartiments, consultez Utilisation des balises de répartition des coûts pour les compartiments S3.	21 août 2012

Modification	Description	Date
Prise en charge des stratégies de compartiment pour l'accès aux API protégé par MFA	Amazon S3 prend désormais en charge l'accès aux API protégé par MFA, une fonctionnalité qui permet d'appliquer l'authentification AWS multifactorielle pour un niveau de sécurité supplémentaire lors de l'accès à vos ressources Amazon S3. Il s'agit d'une fonctionnalité de sécurité qui exige des utilisateurs qu'ils prouvent qu'ils détiennent physiquement un appareil MFA en fournissant un code MFA valide. Pour plus d'informations, consultez Authentification multifacteur AWS. Vous pouvez désormais exiger une authentification MFA pour toutes les demandes d'accès à vos ressources Amazon S3. Pour appliquer l'authentification MFA, Amazon S3 prend désormais en charge la clé `aws:MultiFactorAuthAge` dans une politique de compartiment. Pour un exemple de politique de compartiment, consultez Exigence d'une MFA.	10 juillet 2012
Prise en charge de la fonctionnalité d'expiration d'objet	La fonctionnalité d'expiration d'objet vous permet de planifier la suppression automatique de données une fois écoulé un certain délai. Pour définir l'expiration d'objet, vous ajoutez une configuration de cycle de vie à un compartiment.	27 décembre 2011
Prise en charge d'une nouvelle Région	Amazon S3 prend désormais en charge la Région Amérique du Sud (São Paulo). Pour plus d'informations, consultez Accès à un compartiment à usage général Amazon S3.	14 décembre 2011

Modification	Description	Date
Suppression de plusieurs objets	Amazon S3 prend désormais en charge l'API de suppression de plusieurs objets qui vous permet de supprimer plusieurs objets dans le cadre d'une seule demande. Grâce à cette fonction, vous pouvez supprimer un grand nombre d'objets d'Amazon S3 bien plus rapidement qu'avec plusieurs demandes DELETE individuelles. Pour plus d'informations, consultez Suppression d'objets Amazon S3.	7 décembre 2011
Prise en charge d'une nouvelle Région	Amazon S3 prend désormais en charge la Région USA Ouest (Oregon). Pour plus d'informations, consultez Compartiments et Régions.	8 novembre 2011
Mise à jour de la documentation	Correctifs de la documentation.	8 novembre 2011
Mise à jour de la documentation	En plus des correctifs de la documentation, cette mise à jour offre les améliorations suivantes : • Nouvelles sections de chiffrement côté serveur utilisant le AWS SDK pour PHP et le AWS SDK pour Ruby (voirSpécification du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3)).	17 octobre 2011
Prise en charge du chiffrement côté serveur	Amazon S3 prend désormais en charge le chiffrement côté serveur. Ceci vous permet de demander à Amazon S3 de chiffrer vos données au repos, c'est-à-dire de chiffrer vos données d'objets l'objet lorsqu'Amazon S3 les écrit sur des disques dans ses centres de données. Outre les mises à jour de l'API REST, .NET AWS SDK pour Java et .NET fournissent les fonctionnalités nécessaires pour demander un chiffrement côté serveur. Vous pouvez également demander le chiffrement côté serveur lors du chargement d'objet avec la AWS Management Console. Pour en savoir plus sur le chiffrement des données, consultez Utilisation du chiffrement des données.	4 octobre 2011

Modification	Description	Date
Mise à jour de la documentation	En plus des correctifs de la documentation, cette mise à jour offre les améliorations suivantes : • Des exemples Ruby et PHP ont été ajoutés à la section Envoi de demandes dans la Référence d'API Amazon S3. • Ajout de sections décrivant comment générer et utiliser le pré-signé URLs. Pour plus d'informations, consultez Partage d'objets avec présigné URLs et Partage d'objets avec présigné URLs. • Mise à jour d'une section existante pour présenter AWS les explorateurs pour Eclipse et Visual Studio. Pour plus d'informations, consultez la section Développement avec Amazon S3 AWS SDKs à l'aide du document de référence des API Amazon S3.	22 septembre 201

Modification	Description	Date
Prise en charge des demandes utilisant des informations d’identification de sécurité temporaires	En plus d'utiliser vos informations d'identification de sécurité Compte AWS et celles de l'utilisateur IAM pour envoyer des demandes authentifiées à Amazon S3, vous pouvez désormais envoyer des demandes à l'aide des informations d'identification de sécurité temporaires que vous avez obtenues auprès de AWS Identity and Access Management (IAM). Vous pouvez utiliser l' AWS Security Token Service API ou les bibliothèques d' AWS encapsulation du SDK pour demander ces informations d'identification temporaires à IAM. Vous pouvez demander ces informations d’identification de sécurité temporaires pour votre propre utilisation ou pour les passer à des utilisateurs fédérés et à des applications. Cette fonctionnalité vous permet de gérer vos utilisateurs à l'extérieur AWS et de leur fournir des informations de sécurité temporaires pour accéder à vos AWS ressources. Pour plus d’informations, consultez Envoi de demandes dans la Référence d’API Amazon S3. Pour plus d’informations sur la prise en charge des informations d’identification de sécurité temporaires par IAM, consultez Informations d’identification de sécurité temporaires dans le Guide de l’utilisateur IAM.	3 août 2011

Modification	Description	Date
L'API de chargement partitionné peut désormais copier des objets d'une taille maximale de 5 To	Avant cette mise à jour, l'API Amazon S3 prenait en charge la copie d'objets d'une taille maximale de 5 Go. Pour activer la copie d'objets d'une taille supérieure à 5 Go, Amazon S3 enrichit désormais l'API de chargement partitionné d'une nouvelle opération, `Upload Part (Copy)`. Vous pouvez utiliser cette opération de chargement partitionné pour copier les objets d'une taille maximale de 5 To. Pour plus d'informations, consultez Copie, déplacement et changement de nom des objets. Pour obtenir des informations conceptuelles sur l'API de chargement partitionné, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.	21 juin 2011
Désactivation des appels de l'API SOAP via HTTP	Pour améliorer la sécurité, les appels de l'API SOAP via HTTP ont été désactivés. Les demandes SOAP authentifiées et anonymes doivent être envoyées à Amazon S3 à l'aide de SSL.	6 juin 2011

Modification	Description	Date
IAM permet la délégation entre comptes	Auparavant, pour accéder à une ressource Amazon S3, un utilisateur IAM avait besoin des autorisations du parent Compte AWS et du propriétaire de la ressource Amazon S3. Grâce à l'accès intercompte, l'utilisateur IAM a besoin désormais uniquement de l'autorisation du compte propriétaire. En d'autres termes, si un propriétaire de ressource accorde l'accès à un Compte AWS, il Compte AWS peut désormais accorder à ses utilisateurs IAM l'accès à ces ressources. Pour plus d'informations, consultez Création d'un rôle pour déléguer des autorisations à un utilisateur IAM dans le Guide de l'utilisateur IAM. Pour plus d'informations sur la désignation de mandataires dans une politique de compartiment, consultez Principaux pour les politiques de compartiment.	6 juin 2011
Nouveau lien	Les informations relatives au point de terminaison de ce service sont désormais situées dans la Référence générale AWS . Pour plus d'informations, consultez Régions et points de terminaison dans la Référence générale AWS.	1 mars 2011

Modification	Description	Date
Prise en charge de l'hébergement de sites web statiques dans Amazon S3	Amazon S3 offre désormais une prise en charge améliorée de l'hébergement de sites web statiques. Parmi ces améliorations, citons la prise en charge des documents d'index et des documents d'erreur personnalisés. Lorsque vous utilisez ces fonctions, les demandes effectuées à la racine de votre compartiment ou dans un sous-dossier (par exemple, `http://mywebsite.com/subfolder`) renvoient votre document d'index en lieu et place de la liste des objets contenus dans votre compartiment. En cas d'erreur, Amazon S3 renvoie vos messages d'erreur personnalisés en lieu et place des messages d'erreur d'Amazon S3. Pour plus d'informations, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.	6 juin 2011
Les informations relatives au point de terminaison de ce service sont désormais situées dans la Référence générale AWS . Pour plus d'informations, consultez Régions et points de terminaison dans la Référence générale AWS.	1 mars 2011	

Modification	Description	Date
Prise en charge de l'hébergement de sites web statiques dans Amazon S3	Amazon S3 offre désormais une prise en charge améliorée de l'hébergement de sites web statiques. Parmi ces améliorations, citons la prise en charge des documents d'index et des documents d'erreur personnalisés. Lorsque vous utilisez ces fonctions, les demandes effectuées à la racine de votre compartiment ou dans un sous-dossier (par exemple, `http://mywebsite.com/subfolder`) renvoient votre document d'index en lieu et place de la liste des objets contenus dans votre compartiment. En cas d'erreur, Amazon S3 renvoie vos messages d'erreur personnalisés en lieu et place des messages d'erreur d'Amazon S3. Pour plus d'informations, consultez Hébergement d'un site Web statique à l'aide d'Amazon S3.	17 février 2011
Prise en charge par l'API des en-têtes de réponse	L'API REST de GET Object vous permet désormais de modifier les en-têtes de réponse de la demande GET Object de REST, pour chaque demande. Ainsi, vous pouvez modifier des métadonnées d'objet dans la réponse, sans altérer l'objet lui-même. Pour plus d'informations, consultez Téléchargement d'objets.	14 janvier 2011
Prise en charge des objets volumineux	Amazon S3 a augmenté la taille maximale d'un objet à stocker dans un compartiment S3 : celle-ci passe de 5 Go à 5 To. Si vous utilisez l'API REST, vous pouvez charger des objets de 5 Go maximum en une seule opération PUT. Pour les objets plus volumineux, vous devrez utiliser le chargement partitionné de l'API REST pour charger des objets en plusieurs parties. Pour plus d'informations, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.	9 décembre 2010

Modification	Description	Date
Chargement partitionné	Le chargement partitionné permet des téléchargements plus rapides et plus flexibles sur Amazon S3. Il vous permet de charger un seul objet en tant qu'ensemble de parties. Pour plus d'informations, consultez Chargement et copie d'objets à l'aide du chargement partitionné dans Amazon S3.	10 novembre 2010
Prise en charge de l'ID canonique dans les stratégies de compartiment	Vous pouvez désormais spécifier des règles canoniques IDs dans les compartiments. Pour de plus amples informations, consultez Principaux pour les politiques de compartiment.	17 septembre 2010
Amazon S3 fonctionne avec IAM	Ce service s'intègre désormais à AWS Identity and Access Management (IAM). Pour plus d'informations, consultez Services Services AWS qui fonctionnent avec IAM dans le Guide de l'utilisateur IAM.	2 septembre 2010
Notifications	La fonction de notifications Amazon S3 vous permet de configurer un compartiment afin qu'Amazon S3 publie un message vers une rubrique Amazon Simple Notification Service (Amazon SNS) lorsqu'Amazon S3 détecte un événement clé sur un compartiment. Pour plus d'informations, consultez Configuration de la notification des événements de compartiment.	14 juillet 2010
Politiques de compartiment	Les stratégies de compartiment sont un système de gestion des accès permettant d'accorder des autorisations dans des compartiments, objets et groupes d'objets. Cette fonctionnalité s'ajoute, et dans de nombreux cas, remplace les listes de contrôle d'accès. Pour de plus amples informations, veuillez consulter Politiques de compartiment pour Amazon S3.	6 juillet 2010

Modification	Description	Date
Syntaxe de type chemin disponible dans toutes les Régions	Amazon S3 prend désormais en charge la syntaxe de type chemin pour tout compartiment dans une Région USA classique, ou si le compartiment se trouve dans la même Région, au point de terminaison de la demande. Pour plus d'informations, consultez Hébergement virtuel.	9 juin 2010
Nouveau point de terminaison pour l'Europe (Irlande)	Simple Storage Service (Amazon S3) fournit désormais un point de terminaison pour l'Europe (Irlande) : `http://s3-eu-west-1.amazonaws.com` .	9 juin 2010
console	Vous pouvez maintenant utiliser Simple Storage Service (Amazon S3) via la AWS Management Console. Vous pouvez lire toutes les fonctions d'Amazon S3 dans la console dans le Guide de l'utilisateur Amazon Simple Storage Service.	9 juin 2010
Redondance réduite	Amazon S3 vous permet désormais de réduire vos coûts de stockage en stockant des objets dans Amazon S3, avec moins de redondance. Pour plus d'informations, consultez Stockage à redondance réduite (RRS).	12 mai 2010
Prise en charge d'une nouvelle Région	Amazon S3 prend désormais en charge la Région Asie-Pacifique (Singapour). Pour plus d'informations, consultez Compartiments et Régions.	28 avril 2010
Gestion des versions d'un objet	Cette mise à jour présente la gestion des versions d'objets. Tous les objets peuvent désormais avoir une clé et une version. Lorsque vous activez la gestion des versions pour un compartiment, Amazon S3 confère un ID de version unique à tous les objets qui y sont ajoutés. Cette fonctionnalité permet la récupération en cas de suppressions ou de remplacements involontaires. Pour plus d'informations, consultez Gestion des versions et Utilisation de la gestion des versions.	8 février 2010

Modification	Description	Date
Prise en charge d'une nouvelle Région	Amazon S3 prend désormais en charge la Région USA Ouest (Californie du Nord). Le nouveau point de terminaison pour les demandes relatives à cette région est `s3-us-west-1.amazonaws.com` . Pour plus d'informations, consultez Compartiments et Régions.	2 décembre 2009
AWS SDK pour .NET	AWS fournit désormais des bibliothèques, des exemples de code, des didacticiels et d'autres ressources aux développeurs de logiciels qui préfèrent créer des applications à l'aide d'opérations d'API spécifiques au langage .NET plutôt que REST ou SOAP. Ces bibliothèques fournissent des fonctions de base (non incluses dans REST ou SOAPAPIs), telles que l'authentification des demandes, les nouvelles tentatives de demande et la gestion des erreurs, afin de faciliter le démarrage. Pour plus d'informations sur les bibliothèques et les ressources spécifiques aux langues, consultez la section Développement avec Amazon S3 à l'aide du manuel AWS SDKs de référence des API Amazon S3.	11 novembre 2009

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.