



Guide de l'utilisateur

Amazon S3 sur Outposts



Version de l'API 2006-03-01

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

Amazon S3 sur Outposts: Guide de l'utilisateur

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

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

Table of Contents

Qu'est-ce que S3 sur Outposts ?	1
Comment fonctionne S3 sur Outposts	1
Régions	2
Compartiments	2
Objets	3
Clés	4
Gestion des versions S3	4
ID de version	4
Classe de stockage et chiffrement	5
Politique de compartiment	5
Points d'accès S3 sur Outposts	6
Caractéristiques de S3 sur Outposts	6
Gestion des accès	6
Journalisation et surveillance du stockage	7
Forte cohérence	8
Services connexes	8
Accès à S3 sur Outposts	8
AWS Management Console	9
AWS Command Line Interface	9
AWS SDKs	9
Paiement de S3 sur Outposts	10
Étapes suivantes	10
Configuration de votre Outpost	11
Commandez un nouvel Outpost	11
En quoi S3 on Outposts est-il différent ?	12
Spécifications	12
Opérations d'API prises en charge	13
AWS CLI Commandes Amazon S3 prises en charge par S3 sur Outposts	13
Fonctions Simple Storage Service (Amazon S3) non prises en charge	14
Restrictions réseau	15
Démarrer avec S3 on Outposts	16
Utilisation de la console S3	16
Créer un compartiment, un point d'accès et un point de terminaison.	17
Étapes suivantes	20

Utilisation du SDK AWS CLI et du SDK pour Java	20
Étape 1 : créer un compartiment	21
Étape 2 : Créer un point d'accès	21
Étape 3 : Créer un point de terminaison	22
Étape 4 : Charger un objet dans un compartiment S3 on Outposts	23
Mise en réseau pour S3 on Outposts	24
Sélectionner le type d'accès à votre mise en réseau	24
Accès à vos compartiments et objets S3 on Outposts	25
Gestion des connexions à l'aide d'interfaces réseau Elastic inter-comptes	25
Utilisation des compartiments S3 on Outposts	26
Compartiments	26
Points d'accès	26
Points de terminaison	27
Opérations d'API sur S3 on Outposts	27
Création et gestion de compartiments S3 on Outposts	29
Créer un compartiment	30
Ajout de balises	34
Utilisation des stratégies de compartiment	35
Ajout d'une politique de compartiment	36
Affichage d'une politique de compartiment	38
Suppression d'une politique de compartiment	40
Exemples de politique de compartiment	41
Affichage des compartiments	45
Obtenir un compartiment	47
Suppression de votre compartiment	48
Utilisation des points d'accès	50
Création d'un point d'accès	51
Utilisation d'un alias de type compartiment pour votre point d'accès	52
Visualisation de la configuration du point d'accès	57
Lister les points d'accès	58
Suppression d'un point d'accès	59
Ajout d'une stratégie de point d'accès	60
Visualisation d'une stratégie de point d'accès	62
Utilisation de points de terminaison	63
Création d'un point de terminaison	65
Répertorier les points de terminaison	67

Suppression d'un point de terminaison	68
Utilisation des objets S3 on Outposts	71
Charger un objet	72
Copier un objet	73
Utilisation du AWS SDK pour Java	74
Obtenir un objet	75
Liste des objets	78
Suppression d'objets	82
En utilisant HeadBucket	86
Réalisation d'un chargement partitionné	88
Effectuer le chargement partitionné d'un objet dans un compartiment S3 sur Outposts	89
Copie d'un objet de grande taille dans un compartiment S3 sur Outposts à l'aide du chargement partitionné	91
Générer une liste des parties d'un objet dans un compartiment S3 sur Outposts	94
Récupérer une liste de chargements partitionnés en cours dans un compartiment S3 sur Outposts	95
Utilisation d'une signature présignée URLs	96
Limitation des capacités des URL présignées	97
Utilisateurs habilités à créer une URL présignée	99
Quand S3 on Outposts vérifie-t-il la date et l'heure d'expiration dans une URL présignée ? ...	99
Partage d'objets	100
Chargement d'un objet	105
Amazon S3 sur Outposts avec Amazon EMR local	110
Création d'un compartiment Amazon S3 sur Outposts	111
Premiers pas avec Amazon EMR et Amazon S3 sur Outposts	112
Mise en cache d'autorisation et d'authentification	117
Configuration du cache d'autorisation et d'authentification	118
Validation de la signature SigV4A	118
Sécurité	119
Configuration de IAM	120
Principes des politiques S3 sur Outposts	122
ARNs pour S3 sur Outposts	122
Exemples de stratégies pour S3 sur Outposts	124
Autorisations pour les points de terminaison	124
Rôles lié à un service pour S3 sur Outposts	127
Chiffrement des données	127

AWS PrivateLink pour S3 sur Outposts	127
Restrictions et limitations	129
Accès aux points de terminaison d'interface S3 sur Outposts	129
Mise à jour d'une configuration DNS sur site	131
Création d'un point de terminaison d'un VPC	132
Création de stratégies de point de terminaison de VPC et de stratégies de compartiment	132
Clés de stratégie Signature Version 4 (SigV4)	135
Exemples de stratégies de compartiment qui utilisent des clés de condition associées à Signature Version 4	136
AWS politiques gérées	139
AWSS3OnOutpostsServiceRolePolicy	139
Mises à jour des politiques	139
Utilisation des rôles liés à un service	140
Autorisations de rôle lié à un service pour S3 sur Outposts	141
Création d'un rôle lié à un service pour S3 sur Outposts	144
Modification d'un rôle lié à un service pour S3 sur Outposts	144
Suppression d'un rôle lié à un service pour S3 sur Outposts	144
Régions prises en charge pour les rôles liés à un service S3 sur Outposts	145
Gestion de stockage S3 on Outposts	146
Gestion de la gestion des versions S3	146
Création et gestion d'une configuration de cycle de vie	149
Utilisation de la console	149
Utilisation du SDK AWS CLI et du SDK pour Java	154
Répliquer des objets pour S3 sur Outposts	158
Configuration de réplication	159
Exigences pour la réplication S3 sur Outposts	160
Ce qui est répliqué	160
Ce qui n'est pas répliqué	161
Qu'est-ce qui n'est pas pris en charge par la réplication S3 sur Outposts ?	162
Configuration de la réplication	162
Gestion de votre réplication	183
Partager S3 sur Outposts	192
Prérequis	192
Procédure	193
Exemples d'utilisation	194
Autres services	197

Surveillance de S3 on Outposts	198
CloudWatch métriques	198
CloudWatch métriques	199
CloudWatch Événements Amazon	201
CloudTrail journaux	202
Activation de la CloudTrail journalisation pour S3 sur les objets Outposts	203
Entrées du fichier AWS CloudTrail journal d'Amazon S3 on Outposts	206
Développement avec S3 on Outposts	209
Régions prises en charge	209
S3 sur Outposts APIs	210
Opérations d'API Amazon S3 pour la gestion des objets	210
Opérations d'API de contrôle Amazon S3 pour la gestion des compartiments	211
Opérations d'API S3 sur Outposts pour la gestion d'Outposts	212
Configurer le client de contrôle S3	213
Faire des demandes sur IPv6	213
Commencer avec IPv6	214
Envoi de demandes à l'aide de points de terminaison Dual-Stack	215
Utilisation des IPv6 adresses dans les politiques IAM	216
Test de compatibilité d'adresses IP	217
Utilisation IPv6 avec AWS PrivateLink	218
Utilisation des points de terminaison Dual-Stack	221
.....	ccxxvi

Qu'est-ce que Amazon S3 sur Outposts ?

AWS Outposts est un service entièrement géré qui offre la même AWS infrastructure, les mêmes AWS services et les mêmes outils à pratiquement tous les centres de données, espaces de colocation ou installations sur site pour une expérience hybride véritablement cohérente. APIs AWS Outposts est idéal pour les charges de travail qui nécessitent un accès à faible latence aux systèmes sur site, le traitement local des données, la résidence des données et la migration d'applications avec des interdépendances entre les systèmes locaux. Pour plus d'informations, consultez [Présentation d'AWS Outposts](#) dans le Guide de l'utilisateur AWS Outposts .

Avec Amazon S3 sur Outposts, vous pouvez créer des compartiments S3 sur vos Outposts afin de stocker et récupérer facilement des objets sur site. S3 on Outposts fournit une nouvelle classe de stockage qui utilise Amazon S3 APIs et est conçue pour stocker les données de manière durable et redondante sur plusieurs appareils et serveurs de vos Outposts. OUTPOSTS Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC).

Vous pouvez utiliser les mêmes APIs fonctionnalités sur les compartiments 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 Command Line Interface (AWS CLI) ou REST. AWS SDKs

- [Comment fonctionne S3 sur Outposts](#)
- [Caractéristiques de S3 sur Outposts](#)
- [Services connexes](#)
- [Accès à S3 sur Outposts](#)
- [Paiement de S3 sur Outposts](#)
- [Étapes suivantes](#)

Comment fonctionne S3 sur Outposts

S3 sur Outposts est un service de stockage d'objets qui stocke les données sous forme d'objets dans des compartiments sur votre Outpost. Un objet est un fichier et toutes les métadonnées qui le décrivent. Un compartiment est un conteneur d'objets.

Pour stocker vos données dans S3 sur Outposts, vous devez d'abord créer un compartiment. Lorsque vous créez le compartiment, vous spécifiez un nom de compartiment et l'Outpost qui va contenir le compartiment. Pour accéder à votre compartiment S3 sur Outposts et effectuer des opérations sur les objets, vous devez ensuite créer et configurer un point d'accès. Vous devez également créer un point de terminaison pour router les requêtes vers votre point d'accès.

Les points d'accès simplifient l'accès aux données pour Service AWS toute application cliente qui stocke des données dans S3. Les points d'accès sont des points de terminaison réseau nommés qui sont attachés aux compartiments et peuvent être utilisés pour effectuer des opérations sur les objets, telles que `GetObject` et `PutObject`. Chaque point d'accès dispose d'autorisations et de contrôles réseau distincts.

Vous pouvez créer et gérer vos compartiments, points d'accès et points de terminaison S3 on Outposts à l'aide de l'API AWS Management Console, AWS CLI AWS SDKs, ou REST. Pour télécharger et gérer des objets dans votre compartiment S3 on Outposts, vous pouvez utiliser l'API AWS CLI AWS SDKs, ou l'API REST.

Régions

Pendant le AWS Outposts provisionnement, vous créez ou AWS créez une connexion de liaison de service qui reconnecte votre Outpost à la région de votre choix ou à la région d'origine de l' Région AWS Outpost pour les opérations de bucket et la télémétrie. Un Outpost repose sur la connectivité avec le parent Région AWS. Le rack Outposts n'est pas conçu pour les opérations déconnectées ou les environnements présentant une connectivité limitée ou nulle. Pour obtenir plus d'informations, consultez [Connectivité d'Outpost avec les Régions AWS](#) dans le Guide de l'utilisateur AWS Outposts

Compartiments

Un compartiment est un conteneur pour les objets stockés dans S3 sur Outposts. Vous pouvez stocker un nombre quelconque d'objets dans un compartiment et vous pouvez avoir jusqu'à 100 compartiments par compte et par Outpost.

Lorsque vous créez un compartiment, vous saisissez un nom de compartiment et sélectionnez l'Outpost où le compartiment sera hébergé. Après avoir créé un compartiment, vous ne pouvez pas changer le nom du compartiment ou le déplacer vers un autre Outpost. Les noms de compartiments doivent suivre les [règles de dénomination de compartiment Amazon S3](#). Dans S3 on Outposts, les noms de bucket sont propres à un Outpost et. Compte AWS Les compartiments S3 sur Outposts nécessitent `outpost-id`, `account-id` et le nom du compartiment pour les identifier.

L'exemple suivant montre le format Amazon Resource Name (ARN) pour les compartiments S3 sur Outposts. L'ARN est composé de la région où se trouve votre Outpost, de votre compte Outpost, de l'ID de l'Outpost et du nom du compartiment.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/bucket-name
```

Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'ARN du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN du point d'accès pour S3 sur Outposts, qui inclut l'*outpost-id*, l'*account-id* et le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur les compartiments, consultez [Utilisation des compartiments S3 on Outposts](#).

Objets

Les objets sont les entités fondamentales stockées dans S3 sur Outposts. Les objets sont composés de données et de métadonnées. Les métadonnées sont un ensemble de paires nom-valeur décrivant des objets. Ces paires 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. Un objet est identifié de manière unique dans un compartiment par une clé (ou un nom).

Avec Amazon S3 sur Outposts, les données des objets sont toujours stockées sur l'Outpost. Lorsque vous AWS installez un rack Outpost, vos données restent locales dans votre Outpost afin de répondre aux exigences en matière de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme il AWS Management Console est hébergé dans la région, vous ne pouvez pas utiliser la console pour télécharger ou gérer des objets dans votre Outpost. Cependant, vous pouvez utiliser l'API REST, AWS Command Line Interface (AWS CLI), et AWS SDKs pour télécharger et gérer vos objets via vos points d'accès.

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 et d'un ID de version identifie chaque objet de manière unique.

L'exemple suivant montre le format ARN pour les objets S3 on Outposts, qui inclut le Région AWS code de la région dans laquelle l'Outpost est hébergé, l'ID, l' Compte AWS ID de l'Outpost, le nom du bucket et la clé d'objet :

```
arn:aws:s3-outposts:us-west-2:123456789012:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1/object/myobject
```

Pour en savoir plus sur les clés d'objet, consultez [Utilisation des objets S3 on Outposts](#).

Gestion des versions S3

Vous pouvez utiliser la gestion des versions S3 sur des compartiments Outposts 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. La gestion des versions S3 vous aide à récupérer en cas d'action involontaire d'un utilisateur et de défaillance applicative.

Pour de plus amples informations, veuillez consulter [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#).

ID de version

Lorsque vous activez la gestion des versions S3 pour un compartiment, S3 sur Outposts 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, par exemple [PutObject](#), les nouveaux objets obtiennent un ID de version unique.

Pour de plus amples informations, veuillez consulter [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#).

Classe de stockage et chiffrement

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 AWS Outposts. Si vous essayez d'utiliser d'autres classes de stockage S3 avec S3 sur Outposts, celui-ci renvoie l'erreur `InvalidStorageClass`.

Par défaut, 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 de plus amples informations, veuillez consulter [Chiffrement des données dans S3 sur Outposts](#).

Politique de compartiment

Une politique de compartiment est une politique basée sur les ressources Gestion des identités et des accès AWS (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 stratégies de compartiment utilisent le langage de politique IAM 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 stratégies de compartiment autorisent ou refusent les requêtes en fonction des éléments de la stratégie. Ces éléments peuvent comprendre le demandeur, les actions de S3 sur Outposts, les ressources et les aspects ou conditions de la requête (par exemple, l'adresse IP utilisée pour effectuer la requête). Par exemple, vous pouvez créer une politique de compartiment qui accorde des autorisations inter-comptes pour charger des objets dans un compartiment S3 sur Outposts, tout en veillant à ce que le propriétaire du compartiment ait le contrôle total des objets chargés.

Dans votre politique de compartiment, vous pouvez utiliser des caractères génériques (*) 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 [préfixe](#) courant ou se terminent par une extension donnée, comme `.html`.

Points d'accès S3 sur Outposts

Les points d'accès S3 sur Outposts sont des points de terminaison réseau nommés avec des stratégies d'accès dédiées qui décrivent la manière d'accéder aux données en utilisant ce point de terminaison. Les points d'accès simplifient la gestion de l'accès aux données à grande échelle pour les jeux de données partagés dans S3 sur Outposts. Les points d'accès sont rattachés à des compartiments que vous pouvez utiliser pour effectuer des opérations sur des objets S3, telles que `GetObject` et `PutObject`.

Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'ARN du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

Les points d'accès disposent d'autorisations et de contrôles de réseau distincts que S3 sur Outposts applique pour toute requête effectuée via ce point d'accès. 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 [Accès à vos compartiments et objets S3 on Outposts](#).

Caractéristiques de S3 sur Outposts

Gestion des accès

S3 sur Outposts offre des fonctionnalités d'audit et de gestion de l'accès à vos compartiments et objets. Par défaut, les compartiments S3 sur Outposts et les objets qu'ils contiennent sont privés. Vous n'avez accès qu'aux ressources S3 sur Outposts que vous créez.

Pour accorder des autorisations de ressources granulaires qui prennent en charge votre cas d'utilisation spécifique ou pour auditer les autorisations de vos ressources S3 sur Outposts, vous pouvez utiliser les fonctionnalités suivantes.

- [S3 Block Public Access](#) (Bloquer l'accès public S3) — bloquer l'accès public des compartiments S3 et des objets. Pour les compartiments sur les Outposts, le blocage de l'accès public est toujours activé par défaut.
- [Gestion des identités et des accès AWS \(IAM\)](#) — IAM est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources, y compris à vos ressources S3 on

Outposts. Avec IAM, vous pouvez gérer de manière centralisée les autorisations qui contrôlent les ressources AWS 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.

- [S3 sur Outposts access points](#) (Points d'accès S3 sur Outposts) — Gérez l'accès aux données pour les jeux de données partagés dans S3 sur Outposts. Les points d'accès sont nommés points de terminaison réseau avec des stratégies d'accès dédiées. Les points d'accès sont attachés aux compartiments et peuvent être utilisés pour effectuer des opérations sur les objets, par exemple `GetObject` et `PutObject`.
- [Stratégies 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.
- [AWS Resource Access Manager \(AWS RAM\)](#) — Partagez en toute sécurité votre capacité S3 on Outposts entre Comptes AWS, au sein de votre organisation ou de vos unités organisationnelles (OUs) dans AWS Organizations

Journalisation et surveillance du stockage

S3 sur Outposts fournit des outils de journalisation et de surveillance que vous pouvez utiliser pour surveiller et contrôler l'utilisation de vos ressources S3 sur Outposts. Pour plus d'informations, consultez [Outils de surveillance](#).

- [Amazon CloudWatch Metrics for S3 on Outposts](#) : suivez l'état de fonctionnement de vos ressources et déterminez la disponibilité de vos capacités.
- [CloudWatch Événements Amazon Events pour S3 on Outposts](#) — Créez une règle pour tout événement de l'API S3 on Outposts afin de recevoir des notifications via toutes les cibles d'CloudWatch événements prises en charge, notamment Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) et AWS Lambda
- [AWS CloudTrail journaux pour S3 sur Outposts](#) — Enregistrez les actions effectuées par un utilisateur, un rôle ou une action Service AWS dans S3 sur Outposts. CloudTrail les journaux vous fournissent un suivi détaillé des API pour les opérations au niveau du bucket S3 et au niveau de l'objet.

Forte cohérence

S3 on Outposts fournit une forte read-after-write cohérence pour les requêtes PUT et DELETE des objets de votre bucket S3 on Outposts dans l'ensemble. Régions AWS Ce comportement s'applique à la fois aux écritures de nouveaux objets, aux demandes PUT qui écrasent des objets existants et aux demandes DELETE. En outre, les balises des objets S3 sur Outposts et les métadonnées des objets (par exemple, l'objet HEAD) sont fortement cohérentes. Pour plus d'informations, consultez [Modèle de cohérence des données Amazon S3](#) dans le Guide de l'utilisateur Amazon S3.

Services connexes

Une fois que vous avez chargé vos données dans S3 sur Outposts, vous pouvez les utiliser avec d'autres Services AWS. Les services suivants sont ceux que vous êtes susceptibles d'utiliser le plus fréquemment :

- [Amazon Elastic Compute Cloud \(Amazon EC2\)](#) — offre une capacité de calcul évolutive dans le AWS Cloud. En utilisant Amazon EC2, vous n'avez pas besoin d'investir dans du matériel au départ, ce qui vous permet de développer et de déployer des applications plus rapidement. Vous pouvez utiliser Amazon EC2 pour lancer autant de serveurs virtuels que nécessaire, configurer la sécurité et les réseaux, et gérer le stockage.
- [Amazon Elastic Block Store \(Amazon EBS\) sur Outposts](#) — utilisez les instantanés locaux Amazon EBS sur Outposts pour stocker localement des instantanés de volumes sur un Outpost dans S3 sur Outposts.
- [Amazon Relational Database Service \(Amazon RDS\) sur Outposts](#) – utilisez les sauvegardes locales Amazon RDS pour stocker vos sauvegardes Amazon RDS localement sur votre Outpost.
- [AWS DataSync](#)— Automatisez le transfert de données entre vos Outposts et Régions AWS choisissez les éléments à transférer, le moment du transfert et la quantité de bande passante réseau à utiliser. S3 on Outposts est intégré à AWS DataSync Pour les applications locales nécessitant un traitement local à haut débit, S3 sur Outposts fournit un stockage d'objets sur site afin de minimiser les transferts de données et la mémoire tampon liés aux variations réseau, tout en vous offrant la possibilité de transférer facilement des données entre les Outposts et les Régions AWS.

Accès à S3 sur Outposts

Vous pouvez utiliser S3 sur Outposts de l'une des manières suivantes :

AWS Management Console

La console est une interface utilisateur basée sur le Web pour gérer les S3 sur Outposts et les ressources AWS . Si vous vous êtes inscrit à un Compte AWS, vous pouvez accéder à S3 sur Outposts en vous connectant au AWS Management Console et en choisissant S3 sur la page d'AWS Management Console accueil. Ensuite, choisissez Compartiments Outposts dans le volet de navigation de gauche.

AWS Command Line Interface

Vous pouvez utiliser les outils de ligne de commande AWS 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 est pris en charge sur Windows, macOS et Linux. Consultez le [AWS Command Line Interface Guide de l'utilisateur](#) pour démarrer. Pour obtenir plus d'informations sur les commandes que vous pouvez utiliser avec S3 sur Outposts, consultez les sections [s3api](#), [s3control](#), et [s3outposts](#) 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 sur AWS Outposts et. Comme S3 on Outposts utilise la même solution SDKs qu'Amazon S3, S3 on Outposts fournit une expérience cohérente en utilisant le même S3 APIs, la même automatisation et les mêmes outils.

S3 sur Outposts est un service REST. Vous pouvez envoyer des requêtes à S3 sur Outposts en utilisant les bibliothèques SDK AWS , qui enveloppent l'API REST 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 sur lesquels vous pouvez appuyer AWS](#).

Paiement de S3 sur Outposts

Vous pouvez acheter diverses configurations de AWS Outposts rack comprenant une combinaison de types d'instances Amazon EC2, de volumes de disques SSD () à usage général Amazon EBS () et de S3 gp2 on Outposts. Les prix comprennent la livraison, l'installation et la maintenance des services d'infrastructure, ainsi que les correctifs et mises à niveau logiciels.

Pour de plus amples informations, consultez la rubrique [Tarification de racks AWS Outposts](#).

Étapes suivantes

Pour plus d'informations sur l'utilisation de S3 sur Outposts, consultez les rubriques suivantes :

- [Configuration de votre Outpost](#)
- [En quoi Amazon S3 on Outposts est-il différent de Amazon S3 ?](#)
- [Premiers pas avec Amazon S3 sur Outposts](#)
- [Mise en réseau pour S3 on Outposts](#)
- [Utilisation des compartiments S3 on Outposts](#)
- [Utilisation des objets S3 on Outposts](#)
- [Sécurité dans S3 on Outposts](#)
- [Gestion de stockage S3 on Outposts](#)
- [Développement avec Amazon S3 on Outposts](#)

Configuration de votre Outpost

Pour commencer à utiliser Amazon S3 sur Outposts, vous aurez besoin d'un Outpost avec une capacité Amazon S3 déployée sur votre site d'installation. Pour de plus amples informations sur les options de commande d'une capacité Outpost et S3, veuillez consulter [AWS Outposts](#). Pour vérifier si vos Outposts ont une capacité S3, vous pouvez utiliser l'appel d'API [ListOutpostsWithS3](#). Pour les spécifications et découvrir en quoi S3 on Outposts est différent d'Amazon S3, veuillez consulter [En quoi Amazon S3 on Outposts est-il différent de Amazon S3 ?](#).

Pour plus d'informations, consultez les rubriques suivantes.

Rubriques

- [Commandez un nouvel Outpost](#)

Commandez un nouvel Outpost

Si vous devez commander un nouvel Outpost doté d'une capacité S3, consultez les [tarifs en AWS Outposts rack](#) pour connaître les options de capacité pour Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS) et Amazon S3.

Après avoir sélectionné votre configuration, suivez les étapes décrites dans [Création d'un Outpost et commande de capacité Outpost](#) dans le Guide de l'utilisateur AWS Outposts .

En quoi Amazon S3 on Outposts est-il différent de Amazon S3 ?

Amazon S3 on Outposts fournit un stockage d'objets à votre environnement sur AWS Outposts site. S3 sur Outposts vous aide à répondre aux besoins de traitement local, de résidence des données et de performances exigeantes en maintenant les données à proximité des applications sur site. Parce qu'il utilise Amazon S3 APIs et ses fonctionnalités, S3 on Outposts facilite le stockage, la sécurisation, le balisage, le reporting et le contrôle de l'accès aux données de vos Outposts, ainsi que l'extension de l' AWS infrastructure à vos installations sur site pour une expérience hybride cohérente.

Pour plus d'informations sur le caractère unique de S3 on Outposts, consultez les rubriques suivantes.

Rubriques

- [Spécifications de S3 on Outposts](#)
- [Opérations API prises en charge par S3 sur Outposts](#)
- [AWS CLI Commandes Amazon S3 prises en charge par S3 sur Outposts](#)
- [Fonctions Simple Storage Service \(Amazon S3\) non prises en charge par S3 on Outposts](#)
- [Exigences réseau de S3 on Outposts](#)

Spécifications de S3 on Outposts

- La taille maximale du compartiment Outposts est de 50 To.
- La taille maximale des objets est de 5 To dans les compartiments Outposts.
- Le nombre maximal de compartiments Outposts est de 100 par Compte AWS.
- Les compartiments Outposts sont uniquement accessibles à l'aide de points d'accès et de points de terminaison.
- Le nombre maximal de points d'accès par compartiment Outposts est de 10.
- Les stratégies de point d'accès sont limitées à une taille de 20 Ko.
- Le propriétaire de l'Outpost peut gérer l'accès au sein de votre organisation en AWS Organizations utilisant AWS Resource Access Manager. Tous les comptes qui nécessitent un accès à

Outpost doivent se trouver au sein de la même organisation que le compte propriétaire dans AWS Organizations.

- Le compte propriétaire du compartiment S3 on Outposts est toujours le propriétaire de tous les objets du compartiment.
- Seul le compte propriétaire du compartiment S3 on Outposts peut effectuer des opérations sur le compartiment.
- Les limitations de taille d'objet sont compatibles avec Simple Storage Service (Amazon S3).
- Tous les objets stockés sur S3 sur Outposts sont stockés dans la classe de stockage OUTPOSTS.
- Par défaut, tous les objets stockés dans la classe de stockage OUTPOSTS le sont à l'aide du chiffrement côté serveur avec des clés de chiffrement gérées Amazon S3 (SSE-S3). Vous pouvez également choisir explicitement de stocker des objets en utilisant le chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C).
- S'il n'y a pas assez d'espace pour stocker un objet sur votre Outpost, l'API renvoie une exception de capacité insuffisante (ICE).

Opérations API prises en charge par S3 sur Outposts

Pour obtenir une liste des opérations API prises en charge par S3 on Outposts, voir [Opérations d'API Amazon S3 on Outposts](#).

AWS CLI Commandes Amazon S3 prises en charge par S3 sur Outposts

Les AWS CLI commandes Amazon S3 suivantes sont actuellement prises en charge par Amazon S3 sur Outposts. Pour plus d'informations, consultez la section [Commandes disponibles](#) dans la référence des AWS CLI commandes.

- [cp](#), [mv](#) et [sync](#) dans le même compartiment Outposts, ou entre un environnement local et un compartiment Outposts.
- [ls](#)
- [presign](#)
- [rm](#)

Fonctions Simple Storage Service (Amazon S3) non prises en charge par S3 on Outposts

Les fonctions Simple Storage Service (Amazon S3) suivantes ne sont actuellement pas prises en charge par Simple Storage Service (Amazon S3) sur Outposts. Toute tentative de les utiliser est rejetée.

- Demandes conditionnelles
- Listes de contrôle d'accès (ACLs)
- Partage des ressources cross-origin (CORS)
- Opérations par lot S3
- Rapports d'inventaire S3
- Modification du chiffrement du compartiment par défaut
- Compartiments publics
- Suppression de l'authentification multifacteur (MFA)
- Transitions de cycle de vie S3 (en plus de la suppression d'objets et de l'arrêt des chargements partitionnés incomplets)
- Conservation légale du verrouillage d'objet S3
- Rétention du verrouillage d'objet
- Chiffrement côté serveur avec clés AWS Key Management Service (AWS KMS) (SSE-KMS)
- Contrôle du délai de réplication S3 (S3 RTC)
- Métriques relatives aux CloudWatch demandes Amazon
- Configuration des métriques
- Transfer Acceleration
- Notifications d'événements S3
- Compartiments de type Paiement par le demandeur
- S3 Select
- AWS Lambda événements
- Server access logging (Journalisation des accès au serveur)
- Demandes HTTP POST
- SOAP
- Accès au site web

Exigences réseau de S3 on Outposts

- Pour acheminer les demandes vers un point d'accès S3 on Outposts, vous devez créer et configurer un point de terminaison S3 on Outposts. Les limites suivantes s'appliquent aux points de terminaison pour S3 on Outposts :
 - Chaque cloud privé virtuel (VPC) sur un Outpost peut avoir un point de terminaison associé, et vous pouvez avoir jusqu'à 100 points de terminaison par Outpost.
 - Vous pouvez mapper plusieurs points d'accès au même point de terminaison.
 - Vous pouvez ajouter des points de terminaison uniquement à VPCs des blocs CIDR dans les sous-espaces des plages CIDR suivantes :
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16
 - Vous pouvez créer des points de terminaison vers un avant-poste uniquement à partir de blocs CIDR VPCs ne se chevauchant pas.
 - Vous ne pouvez créer un point de terminaison qu'à partir de son sous-réseau Outposts.
 - Le sous-réseau que vous utilisez pour créer un point de terminaison doit contenir quatre adresses IP que S3 on Outposts peut utiliser.
 - Si vous spécifiez le groupe d'adresses IP clients (groupe CoIP), il doit contenir quatre adresses IP que S3 on Outposts peut utiliser.
 - Vous ne pouvez créer qu'un point de terminaison par Outpost et par VPC.

Premiers pas avec Amazon S3 sur Outposts

Avec Amazon S3 sur Outposts, vous pouvez créer des compartiments S3 sur votre AWS Outposts afin de stocker et récupérer facilement des objets sur site pour des applications qui nécessitent un accès aux données locales, un traitement local des données et une résidence des données. S3 sur Outposts propose une nouvelle classe de stockage, appelée S3 Outposts (OUTPOSTS), qui utilise les API Amazon S3 et est conçue pour stocker de manière durable et redondante des données sur plusieurs appareils et serveurs sur vos AWS Outposts. Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes API et fonctions sur vos compartiments Outpost que sur les compartiments Amazon S3, telles que les stratégies d'accès, le chiffrement et le balisage. Vous pouvez utiliser S3 sur Outposts via la AWS Management Console, l'AWS Command Line Interface (AWS CLI), des kits SDK AWS ou une API REST.

Avec Amazon S3 sur Outposts, vous pouvez utiliser les API et fonctions Amazon S3, telles que le stockage d'objets, les stratégies d'accès, le chiffrement et le balisage, sur AWS Outposts comme vous le faites sur Amazon S3. Pour de plus amples informations sur S3 on Outposts, veuillez consulter [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Rubriques

- [Commencer par utiliser le AWS Management Console](#)
- [Commencer à utiliser le SDK AWS CLI and pour Java](#)

Commencer par utiliser le AWS Management Console

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur APIs les compartiments Outpost que sur les compartiments 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 Command Line

Interface (AWS CLI) ou REST. AWS SDKs Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Pour commencer à utiliser S3 sur Outposts à l'aide de la console, consultez les rubriques suivantes. Pour commencer à utiliser le AWS CLI ou AWS SDK pour Java, voir [Commencer à utiliser le SDK AWS CLI and pour Java](#).

Rubriques

- [Créer un compartiment, un point d'accès et un point de terminaison.](#)
- [Étapes suivantes](#)

Créer un compartiment, un point d'accès et un point de terminaison.

La procédure suivante vous montre comment créer votre premier compartiment dans S3 sur Outposts. Lorsque vous créez un compartiment à l'aide de la console, vous créez également un point d'accès et un point de terminaison associés au compartiment afin que vous puissiez immédiatement commencer à stocker des objets dans 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 Outposts buckets (Compartiments Outposts).
3. Sélectionnez Create Outposts bucket (Créer un compartiment Outposts).
4. Dans Bucket name (Nom du compartiment), saisissez un nom compatible avec le système de nom de domaine (DNS) pour votre compartiment.

Le nom du compartiment doit présenter les caractéristiques suivantes :

- Soyez unique au sein de Compte AWS l'avant-poste et de l'endroit Région AWS où l'avant-poste est hébergé.
- Il doit comprendre de 3 à 63 caractères.
- Ne contient pas de majuscules.
- Il doit commencer par une minuscule ou un chiffre.

Une fois le compartiment créé, vous ne pouvez pas changer son nom. Pour plus d'informations sur la dénomination des compartiments, consultez [Règles de dénomination des compartiments à usage général](#) dans le Guide de l'utilisateur Amazon S3.

⚠ Important

Évitez d'inclure des 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.

5. Pour Outpost, choisissez l'Outpost où vous souhaitez que le compartiment réside.
6. Sous Bucket Versioning (Gestion des versions du compartiment), définissez l'état de gestion des versions S3 pour votre compartiment S3 sur Outposts sur l'une des options suivantes :
 - Disable (Désactiver) (par défaut) : le compartiment reste non versionné.
 - Enable (Activer) : active la gestion des versions S3 pour les objets du compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique.

Pour plus d'informations sur la gestion des versions S3, consultez [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#).

7. (Facultatif) Ajoutez les balises facultatives que vous souhaitez associer au compartiment Outposts. Vous pouvez utiliser des balises pour suivre des critères pour des projets individuels ou des groupes de projets, ou pour étiqueter vos compartiments en utilisant des balises de répartition des coûts.

Par défaut, tous les objets stockés dans votre compartiment Outposts le sont à l'aide du chiffrement côté serveur avec les clés de chiffrement gérées Amazon S3 (SSE-S3). Vous pouvez également choisir explicitement de stocker des objets en utilisant le chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C). Pour modifier le type de chiffrement, vous devez utiliser l'API REST, AWS Command Line Interface (AWS CLI) ou AWS SDKs.

8. Dans la section Paramètres du point d'accès des Outposts, entrez le nom du point d'accès.

Les points d'accès S3 on Outpost simplifient la gestion de l'accès aux données à grande échelle pour les jeux de données partagés dans S3 on Outpost. Les points d'accès sont des points de terminaison réseau associés à des compartiments Outposts que vous pouvez utiliser pour effectuer des opérations d'objet S3. Pour de plus amples informations, veuillez consulter [Points d'accès](#).

Les noms des points d'accès doivent être uniques dans le compte pour cette région et cet Outpost, mais aussi être conformes aux [restrictions et limitations des points d'accès](#).

9. Choisissez le VPC pour ce point d'accès Amazon S3 sur Outposts.

Si vous n'avez pas de VPC, choisissez [Create VPC \(Créer un VPC\)](#). Pour plus d'informations, consultez [Création de points d'accès restreints à un cloud privé virtuel \(VPC\)](#) dans le Guide de l'utilisateur Amazon S3.

Un cloud privé virtuel (VPC) vous permet de lancer des ressources AWS dans un réseau virtuel défini par vos soins. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d'AWS.

10. (Opération facultative pour un VPC existant) Choisissez un sous-réseau de point de terminaison pour votre point de terminaison.

Un sous-réseau est une plage d'adresses IP dans votre VPC. Si vous ne disposez pas du sous-réseau que vous voulez, sélectionnez [Create subnet \(Créer un sous-réseau\)](#). Pour de plus amples informations, veuillez consulter [Mise en réseau pour S3 on Outposts](#).

11. (Opération facultative pour un VPC existant) Choisissez un groupe de sécurité de point de terminaison pour votre point de terminaison.


Un [groupe de sécurité](#) agit en tant que pare-feu virtuel afin de contrôler le trafic entrant et sortant.

12. (Opération facultative pour un VPC existant) Choisissez le Type d'accès au point de terminaison :

- Private (Privé) — à utiliser avec le VPC.
- Customer owned IP (IP appartenant au client) – À utiliser avec un groupe d'adresses IP appartenant au client (groupe CoIP) au sein de votre réseau sur site.

13. (Facultatif) Spécifiez la stratégie de point d'accès à l'Outpost. La console affiche automatiquement le nom Amazon Resource Name (ARN) du point d'accès, que vous pouvez utiliser dans la stratégie.

14. Sélectionnez [Create Outposts bucket \(Créer un compartiment Outposts\)](#).

 Note

Cela peut prendre jusqu'à 5 minutes pour que votre point de terminaison Outpost soit créé et que votre compartiment soit prêt à l'emploi. Pour configurer des paramètres de compartiment supplémentaires, sélectionnez [Afficher les détails](#).

Étapes suivantes

Avec Amazon S3 sur Outposts, les données des objets sont toujours stockées sur l'Outpost. Lorsque vous installez un rack Outpost, vos données restent locales dans votre Outpost afin de répondre aux exigences de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans une Région AWS. Comme l'AWS Management Console est hébergé dans la région, vous ne pouvez pas utiliser la console pour télécharger ou gérer des objets dans votre Outpost. Cependant, vous pouvez utiliser l'API REST, l'AWS Command Line Interface (AWS CLI), et les AWS SDKs pour télécharger et gérer vos objets via vos points d'accès.

Après avoir créé un compartiment, un point d'accès et un point de terminaison S3 on Outposts, vous pouvez utiliser le SDK for Java AWS CLI ou le SDK pour Java pour télécharger un objet dans votre compartiment. Pour de plus amples informations, veuillez consulter [Chargement d'un objet dans un compartiment S3 sur Outposts](#).

Commencer à utiliser le SDK AWS CLI and pour Java

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise les API Amazon S3 et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur les API des compartiments Outpost que sur les compartiments Amazon S3, notamment les politiques d'accès, le chiffrement et le balisage. Vous pouvez utiliser S3 sur Outposts via l'API AWS Management Console, l'AWS Command Line Interface (AWS CLI) ou REST. Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Pour démarrer avec S3 on Outposts, vous devez créer un compartiment, un point d'accès et un point de terminaison. Ensuite, vous pouvez charger des objets dans votre compartiment. Les exemples suivants vous montrent comment démarrer avec S3 sur Outposts à l'aide du SDK AWS CLI and pour Java. Pour commencer à utiliser la console, veuillez consulter [Commencer par utiliser le AWS Management Console](#).

Rubriques

- [Étape 1 : créer un compartiment](#)

- [Étape 2 : Créer un point d'accès](#)
- [Étape 3 : Créer un point de terminaison](#)
- [Étape 4 : Charger un objet dans un compartiment S3 on Outposts](#)

Étape 1 : créer un compartiment

Les exemples suivants, AWS CLI ainsi que ceux du SDK pour Java, vous montrent comment créer un bucket S3 on Outposts.

AWS CLI

Exemple

L'exemple suivant crée un compartiment S3 sur Outposts (`s3-outposts:CreateBucket`) à l'aide d' AWS CLI. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control create-bucket --bucket example-outposts-bucket --outpost-id op-01ac5d28a6a232904
```

SDK for Java

Exemple

Pour des exemples de création d'un bucket S3 Outposts avec le AWS SDK pour Java, consultez [CreateOutpostsBucket.java dans les exemples de code du SDK pour AWS Java 2.x](#).

Étape 2 : Créer un point d'accès

Pour accéder à votre compartiment Amazon S3 sur Outposts, vous devez créer et configurer un point d'accès. Ces exemples vous montrent comment créer un point d'accès à l'aide du SDK AWS CLI et du SDK pour Java.

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 points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet Amazon S3, notamment `GetObject` et `PutObject`. Avec S3 on Outposts, vous devez utiliser des points

d'accès pour accéder à tout objet dans un compartiment Outposts. Les points d'accès ne prennent en charge que l' virtual-host-styleadressage.

AWS CLI

Exemple

L' AWS CLI exemple suivant crée un point d'accès pour un bucket Outposts. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control create-access-point --account-id 123456789012
--name example-outposts-access-point --bucket "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket" --vpc-configuration VpcId=example-vpc-12345
```

SDK for Java

Exemple

Pour des exemples de création d'un point d'accès pour un bucket S3 Outposts avec le AWS SDK pour Java, consultez [CreateOutpostsAccessPoint.java dans les exemples de code du SDK pour AWS Java 2.x](#).

Étape 3 : Créer un point de terminaison

Pour acheminer les demandes vers un point d'accès Amazon S3 sur Outposts, vous devez créer et configurer un point de terminaison S3 sur Outposts. Pour créer un point de terminaison, vous devrez disposer d'une connexion active avec votre lien de service vers votre région d'accueil Outpost. Chaque cloud privé virtuel (VPC) sur votre Outpost peut avoir un point de terminaison associé. Pour plus d'informations sur les quotas de points de terminaison, consultez [Exigences réseau de S3 on Outposts](#). Vous devez créer un point de terminaison pour pouvoir accéder à vos compartiments Outpost et effectuer des opérations d'objet. Pour de plus amples informations, veuillez consulter [Points de terminaison](#).

Ces exemples vous montrent comment créer un point de terminaison à l'aide du SDK AWS CLI et du SDK pour Java. Pour de plus amples informations sur les autorisations requises pour créer et gérer des points de terminaison, veuillez consulter [Autorisations pour les points de terminaison S3 sur Outposts](#).

AWS CLI

Exemple

L' AWS CLI exemple suivant crée un point de terminaison pour un Outpost en utilisant le type d'accès aux ressources VPC. Le VPC est dérivé du sous-réseau. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id  
subnet-8c7a57c5 --security-group-id sg-ab19e0d1
```

L' AWS CLI exemple suivant crée un point de terminaison pour un Outpost en utilisant le type d'accès au pool d'adresses IP (pool CoIP) appartenant au client. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id  
subnet-8c7a57c5 --security-group-id sg-ab19e0d1 --access-type CustomerOwnedIp --  
customer-owned-ip-v4-pool ipv4pool-coip-12345678901234567
```

SDK for Java

Exemple

Pour des exemples de création d'un point de terminaison pour un Outpost S3 avec le AWS SDK pour Java, [CreateOutpostsEndPointconsultez](#) .java dans les exemples de code du SDK AWS pour Java 2.x.

Étape 4 : Charger un objet dans un compartiment S3 on Outposts

Pour charger un objet, consultez [Chargement d'un objet dans un compartiment S3 sur Outposts](#)

Mise en réseau pour S3 on Outposts

Vous pouvez utiliser Amazon S3 on Outposts pour stocker et récupérer des objets sur site pour les applications qui nécessitent un accès local aux données, un traitement des données et une résidence des données. Cette section décrit les exigences de mise en réseau pour accéder à S3 on Outposts.

Rubriques

- [Sélectionner le type d'accès à votre mise en réseau](#)
- [Accès à vos compartiments et objets S3 on Outposts](#)
- [Interfaces réseau élastiques inter-comptes](#)

Sélectionner le type d'accès à votre mise en réseau

Vous pouvez accéder à S3 sur Outposts à partir d'un VPC ou de votre réseau local. Vous communiquez avec votre compartiment Outpost en utilisant un point d'accès et une connexion de terminaison. Cette connexion maintient le trafic entre votre VPC et vos compartiments S3 on Outposts au sein du réseau AWS . Lorsque vous créez un point de terminaison, vous devez spécifier le type d'accès du point de terminaison, soit `Private` (pour le routage VPC), soit `CustomerOwnedIp` (pour un pool d'adresses IP appartenant au client [pool CoIP]).

- `Private` (pour le routage VPC) — si vous ne spécifiez pas le type d'accès, S3 on Outposts utilise `Private` par défaut. Avec le type d'accès `Private`, les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les ressources de votre Outpost. Vous pouvez travailler avec S3 on Outposts à partir d'un VPC. Ce type de point de terminaison est accessible depuis votre réseau sur site via un routage VPC direct. Pour en savoir plus, consultez [Tables de routage de passerelle locale](#) dans le Guide de l'utilisateur AWS Outposts.
- `CustomerOwnedIp` (pour le pool CoIP) — si vous ne choisissez pas le type d'accès `Private` par défaut et sélectionnez `CustomerOwnedIp`, vous devez spécifier une plage d'adresses IP. Vous pouvez utiliser ce type d'accès pour travailler avec S3 on Outposts à partir de votre réseau sur site et au sein d'un VPC. Lorsque vous accédez à S3 sur Outposts dans un VPC, votre trafic est limité à la bande passante de la passerelle locale.

Accès à vos compartiments et objets S3 on Outposts

Pour accéder à vos compartiments et objets S3 sur Outposts, vous devez disposer des éléments suivants :

- Un point d'accès pour le VPC.
- Un point de terminaison pour le même VPC.
- Une connexion active entre votre Outpost et votre Région AWS. Pour plus d'informations sur la façon de connecter votre Outpost à une région, consultez la section [Connectivité d'Outpost aux AWS régions](#) dans le Guide de l'utilisateur d'AWS Outposts.

Pour plus d'informations sur l'accès aux compartiments et aux objets dans S3 on Outposts, consultez [Utilisation des compartiments S3 on Outposts](#) et [Utilisation des objets S3 on Outposts](#).

Interfaces réseau élastiques inter-comptes

Les points de terminaison S3 on Outposts sont des ressources nommées avec Amazon Resource Names (ARNs). Lorsque ces points de terminaison sont créés, AWS Outposts configure plusieurs interfaces réseau élastiques entre comptes. Les interfaces réseau Elastic de S3 sur Outposts ressemblent aux autres interfaces réseau à une exception près : S3 sur Outposts associe les interfaces réseau Elastic inter-comptes aux instances Amazon EC2.

Le système de noms de domaine (DNS) de S3 sur Outposts équilibre les charges de vos demandes sur l'interface réseau Elastic inter-comptes. S3 on Outposts crée dans votre compte l'interface Elastic network AWS inter-comptes qui est visible depuis le volet Network interfaces de la console Amazon EC2.

Pour les points de terminaison qui utilisent le type d'accès du groupe CoIP, S3 sur Outposts alloue et associe les adresses IP à l'interface réseau Elastic inter-comptes à partir du groupe CoIP configuré.

Utilisation des compartiments S3 on Outposts

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur votre ordinateur AWS Outposts et facilement 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous pouvez utiliser les mêmes APIs fonctionnalités sur les compartiments Outpost que sur Amazon S3, notamment les politiques d'accès, le chiffrement et le balisage. Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Vous communiquez avec vos compartiments Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Pour accéder à vos compartiments et objets S3 on Outposts, vous devez disposer d'un point d'accès pour le VPC et d'un point de terminaison pour le même VPC. Pour de plus amples informations, veuillez consulter [Mise en réseau pour S3 on Outposts](#).

Compartiments

Dans S3 on Outposts, les noms de compartiment sont propres à un avant-poste et nécessitent le Région AWS code de la région dans laquelle l'avant-poste est hébergé, l' Compte AWS identifiant, l'identifiant de l'avant-poste et le nom du compartiment pour les identifier.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/bucket/bucket-name
```

Pour de plus amples informations, veuillez consulter [Ressource ARNs pour S3 sur les Outposts](#).

Points d'accès

Amazon S3 sur Outposts prend en charge les points d'accès Virtual Private Cloud (VPC) uniquement comme seul moyen d'accéder à vos compartiments Outposts.

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 points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet Amazon S3, notamment GetObject et PutObject. Avec S3 on Outposts, vous devez utiliser des points

d'accès pour accéder à tout objet dans un compartiment Outposts. Les points d'accès ne prennent en charge que l' virtual-host-styleadressage.

L'exemple suivant montre le format ARN que vous utilisez pour les points d'accès S3 sur Outposts. L'ARN du point d'accès inclut le Région AWS code de la région dans laquelle l'avant-poste est hébergé, l' Compte AWS identifiant, l'identifiant de l'avant-poste et le nom du point d'accès.

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Points de terminaison

Pour acheminer les demandes vers un point d'accès S3 on Outposts, vous devez créer et configurer un point de terminaison S3 on Outposts. Grâce aux points de terminaison S3 sur Outposts, vous pouvez connecter votre VPC en privé à votre compartiment Outpost. Les points de terminaison S3 on Outposts sont des identificateurs de ressources uniformes virtuels (URLs) du point d'entrée de votre bucket S3 on Outposts. Il s'agit de composants VPC mis à l'échelle horizontalement, redondants et hautement disponibles.

Chaque cloud privé virtuel (VPC) sur votre Outpost peut avoir un point de terminaison associé, et vous pouvez avoir jusqu'à 100 points de terminaison par Outpost. Vous devez créer ces points de terminaison pour pouvoir accéder à vos compartiments Outpost et effectuer des opérations d'objet. Créer ces points de terminaison permet également au modèle d'API et aux comportements d'être les mêmes en permettant aux mêmes opérations de fonctionner dans S3 et S3 sur Outposts.

Opérations d'API sur S3 on Outposts

Pour gérer les opérations d'API de compartiment Outpost, S3 sur Outposts héberge un point de terminaison distinct du point de terminaison Amazon S3. Ce point de terminaison est `s3-outposts.region.amazonaws.com`.

Pour utiliser les opérations d'API de Amazon S3, vous devez signer le compartiment et les objets en utilisant le format ARN correct. Vous devez passer ARNs aux opérations d'API afin qu'Amazon S3 puisse déterminer si la demande concerne Amazon S3 (`s3-control.region.amazonaws.com`) ou S3 on Outposts (`s3-outposts.region.amazonaws.com`). En fonction du format ARN, S3 peut signer et acheminer la demande de manière appropriée.

Chaque fois qu'une demande est envoyée au plan de contrôle Amazon S3, le kit SDK extrait les composants de l'ARN et inclut un en-tête supplémentaire « `x-amz-outpost-id` » avec la valeur

du « *outpost-id* » extrait de l'ARN. Le nom de service de l'ARN est utilisé pour signer la demande avant qu'elle ne soit acheminée vers le point de terminaison S3 on Outposts. Ce comportement s'applique à toutes les opérations d'API gérées par le client `s3control`.

Le tableau suivant répertorie les opérations d'API étendues pour Amazon S3 sur Outposts et leurs modifications par rapport à Amazon S3.

API	Valeur de paramètre S3 sur Outposts	
CreateBucket	Nom de compartiment en tant qu'ARN, ID Outpost	
ListRegionalBuckets	ID Outpost	
DeleteBucket	Nom de compartiment en tant qu'ARN	
DeleteBucketLifecycleConfiguration	Nom de compartiment en tant qu'ARN	
GetBucketLifecycleConfiguration	Nom de compartiment en tant qu'ARN	
PutBucketLifecycleConfiguration	Nom de compartiment en tant qu'ARN	
GetBucketPolicy	Nom de compartiment en tant qu'ARN	
PutBucketPolicy	Nom de compartiment en tant qu'ARN	
DeleteBucketPolicy	Nom de compartiment en tant qu'ARN	
GetBucketTagging	Nom de compartiment en tant qu'ARN	

API	Valeur de paramètre S3 sur Outposts	
PutBucketTagging	Nom de compartiment en tant qu'ARN	
DeleteBucketTagging	Nom de compartiment en tant qu'ARN	
CreateAccessPoint	Nom du point d'accès en tant qu'ARN	
DeleteAccessPoint	Nom du point d'accès en tant qu'ARN	
GetAccessPoint	Nom du point d'accès en tant qu'ARN	
GetAccessPoint	Nom du point d'accès en tant qu'ARN	
ListAccessPoints	Nom du point d'accès en tant qu'ARN	
PutAccessPointPolicy	Nom du point d'accès en tant qu'ARN	
GetAccessPointPolicy	Nom du point d'accès en tant qu'ARN	
DeleteAccessPointPolicy	Nom du point d'accès en tant qu'ARN	

Création et gestion de compartiments S3 on Outposts

Pour plus d'informations sur la création et la gestion des compartiments S3 on Outposts, consultez les rubriques suivantes.

Création d'un compartiment S3 sur Outposts

Avec Amazon S3 sur Outposts, vous pouvez créer des compartiments S3 sur votre AWS Outposts afin de stocker et récupérer facilement des objets sur site pour des applications qui nécessitent un accès aux données locales, un traitement local des données et une résidence des données. S3 sur Outposts propose une nouvelle classe de stockage, appelée S3 Outposts (OUTPOSTS), qui utilise les API Amazon S3 et est conçue pour stocker de manière durable et redondante des données sur plusieurs appareils et serveurs sur vos AWS Outposts. Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes API et fonctions sur vos compartiments Outpost que sur les compartiments Amazon S3, telles que les stratégies d'accès, le chiffrement et le balisage. Vous pouvez utiliser S3 sur Outposts via la AWS Management Console, l'AWS Command Line Interface (AWS CLI), des kits AWS SDK ou une API REST. Pour plus d'informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#)

Note

Le Compte AWS qui crée le compartiment en est le propriétaire et lui peut y valider des actions. Les compartiments possèdent des propriétés de configuration telles que Outpost, balise, chiffrement par défaut et paramètres de point d'accès. Les paramètres du point d'accès comprennent le cloud privé virtuel (VPC), la stratégie du point d'accès pour accéder aux objets du compartiment et d'autres métadonnées. Pour plus d'informations, consultez [Spécifications de S3 on Outposts](#).

Si vous souhaitez créer un compartiment qui utilise AWS PrivateLink pour fournir un accès à la gestion des compartiments et des points de terminaison via les points de terminaison d'un VPC d'interface dans votre cloud privé virtuel (VPC), consultez [AWS PrivateLink pour S3 sur Outposts](#).

Les exemples suivants vous montrent comment créer un compartiment S3 sur Outposts à l'aide d'AWS Management Console, d'AWS Command Line Interface (AWS CLI) et du kit AWS SDK pour Java.

Utilisation de la console S3


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

2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Sélectionnez Create Outposts bucket (Créer un compartiment Outposts).
4. Dans Bucket name (Nom du compartiment), saisissez un nom compatible avec le système de nom de domaine (DNS) pour votre compartiment.

Le nom du compartiment doit présenter les caractéristiques suivantes :

- Être unique au sein du Compte AWS, de l'Outpost et de la Région AWS où se trouve l'Outpost.
- Il doit comprendre de 3 à 63 caractères.
- Ne contient pas de majuscules.
- Il doit commencer par une minuscule ou un chiffre.

Une fois le compartiment créé, vous ne pouvez pas changer son nom. Pour plus d'informations sur la dénomination des compartiments, consultez [Règles de dénomination des compartiments à usage général](#) dans le Guide de l'utilisateur Amazon S3.

 Important

Évitez d'inclure des informations sensibles, notamment des numéros de compte, dans le nom du compartiment. Le nom de compartiment est visible dans les URL qui pointent vers les objets du compartiment.

5. Pour Outpost, choisissez l'Outpost où vous souhaitez que le compartiment réside.
6. Sous Bucket Versioning (Gestion des versions du compartiment), définissez l'état de gestion des versions S3 pour votre compartiment S3 sur Outposts sur l'une des options suivantes :
 - Disable (Désactiver) (par défaut) : le compartiment reste non versionné.
 - Enable (Activer) : active la gestion des versions S3 pour les objets du compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique.

Pour plus d'informations sur la gestion des versions S3, consultez [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#).

7. (Facultatif) Ajoutez les balises facultatives que vous souhaitez associer au compartiment Outposts. Vous pouvez utiliser des balises pour suivre des critères pour des projets individuels

ou des groupes de projets, ou pour étiqueter vos compartiments en utilisant des balises de répartition des coûts.

Par défaut, tous les objets stockés dans votre compartiment Outposts le sont à l'aide du chiffrement côté serveur avec les clés de chiffrement gérées Amazon S3 (SSE-S3). Vous pouvez également choisir explicitement de stocker des objets en utilisant le chiffrement côté serveur avec des clés de chiffrement fournies par le client (SSE-C). Pour modifier le type de chiffrement, vous devez utiliser l'API REST, AWS Command Line Interface (AWS CLI), ou les kits SDK AWS.

8. Dans la section Paramètres du point d'accès des Outposts, entrez le nom du point d'accès.

Les points d'accès S3 on Outpost simplifient la gestion de l'accès aux données à grande échelle pour les jeux de données partagés dans S3 on Outpost. Les points d'accès sont des points de terminaison réseau associés à des compartiments Outposts que vous pouvez utiliser pour effectuer des opérations d'objet S3. Pour plus d'informations, consultez [Points d'accès](#).

Les noms des points d'accès doivent être uniques dans le compte pour cette région et cet Outpost, mais aussi être conformes aux [restrictions et limitations des points d'accès](#).

9. Choisissez le VPC pour ce point d'accès Amazon S3 sur Outposts.

Si vous n'avez pas de VPC, choisissez Create VPC (Créer un VPC). Pour plus d'informations, consultez [Création de points d'accès restreints à un cloud privé virtuel \(VPC\)](#) dans le Guide de l'utilisateur Amazon S3.

Un cloud privé virtuel (VPC) vous permet de lancer des ressources AWS dans un réseau virtuel défini par vos soins. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d'AWS.

10. (Opération facultative pour un VPC existant) Choisissez un sous-réseau de point de terminaison pour votre point de terminaison.

Un sous-réseau est une plage d'adresses IP dans votre VPC. Si vous ne disposez pas du sous-réseau que vous voulez, sélectionnez Create subnet (Créer un sous-réseau). Pour plus d'informations, consultez [Mise en réseau pour S3 on Outposts](#).

11. (Opération facultative pour un VPC existant) Choisissez un groupe de sécurité de point de terminaison pour votre point de terminaison.

Un [groupe de sécurité](#) agit en tant que pare-feu virtuel afin de contrôler le trafic entrant et sortant.

12. (Opération facultative pour un VPC existant) Choisissez le Type d'accès au point de terminaison :
 - Private (Privé) — à utiliser avec le VPC.
 - Customer owned IP (IP appartenant au client) – À utiliser avec un groupe d'adresses IP appartenant au client (groupe ColP) au sein de votre réseau sur site.
13. (Facultatif) Spécifiez la stratégie de point d'accès à l'Outpost. La console affiche automatiquement le nom Amazon Resource Name (ARN) du point d'accès, que vous pouvez utiliser dans la stratégie.
14. Sélectionnez Create Outposts bucket (Créer un compartiment Outposts).

Note

Cela peut prendre jusqu'à 5 minutes pour que votre point de terminaison Outpost soit créé et que votre compartiment soit prêt à l'emploi. Pour configurer des paramètres de compartiment supplémentaires, sélectionnez Afficher les détails.

Utilisation de la AWS CLI

Exemple

L'exemple suivant crée un compartiment S3 sur Outposts (`s3-outposts:CreateBucket`) à l'aide d'AWS CLI. Pour exécuter cette commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3control create-bucket --bucket example-outposts-bucket --outpost-id op-01ac5d28a6a232904
```

Utilisation du kit AWS SDK pour Java

Exemple

Pour des exemples de création d'un compartiment S3 Outposts avec le kit AWS SDK pour Java, consultez [CreateOutpostsBucket.java](#) dans les Exemples de code du kit AWS SDK pour Java 2.x.

Ajout de balises pour les compartiments Amazon S3 on Outposts

Vous pouvez ajouter des balises pour vos compartiments Amazon S3 on Outposts afin de suivre les coûts de stockage ou d'autres critères pour des projets individuels ou des groupes de projets.

Note

Le compte Compte AWS qui crée le compartiment en est le propriétaire, et lui seul peut modifier ses étiquettes.

Utilisation de la console S3

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts dont vous souhaitez modifier les balises.
4. Choisissez l'onglet Propriétés.
5. Sous Balises, choisissez Modifier.
6. Sélectionnez Add new tag (Ajouter une nouvelle balise), puis remplissez le champ Key (Clé) et le champ facultatif Value (Valeur).

Ajoutez les balises que vous souhaitez associer à un compartiment Outposts afin de suivre d'autres critères pour des projets individuels ou des groupes de projets.

7. Sélectionnez Save Changes.

Utilisation de l'AWS CLI

L'exemple AWS CLI suivant applique une configuration de balisage à un compartiment S3 on Outposts en utilisant un document JSON dans le dossier actuel qui spécifie les balises (*tagging.json*). Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

```
aws s3control put-bucket-tagging --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket --tagging file://tagging.json
```

tagging.json

```
{
  "TagSet": [
    {
      "Key": "organization",
      "Value": "marketing"
    }
  ]
}
```

L'exemple AWS CLI suivant applique une configuration de balisage à un compartiment S3 on Outposts directement depuis la ligne de commande.

```
aws s3control put-bucket-tagging --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --tagging 'TagSet=[{Key=organization,Value=marketing}]'
```

Pour de plus amples informations sur cette commande, veuillez consulter [put-bucket-tagging](#) dans le document AWS CLI Reference.

Gestion de l'accès à un compartiment Amazon S3 on Outposts à l'aide d'une stratégie de compartiment

Une politique de compartiment est une politique basée sur les ressources Gestion des identités et des accès AWS (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. Pour de plus amples informations, veuillez consulter [Politique de compartiment](#).

Vous pouvez mettre à jour votre politique de compartiment pour gérer l'accès à votre compartiment Amazon S3 on Outposts. Pour plus d'informations, consultez les rubriques suivantes.

Rubriques

- [Ajout ou modification d'une politique de compartiment pour un compartiment Amazon S3 on Outposts](#).

- [Affichage de la politique de compartiment pour votre compartiment Amazon S3 on Outposts.](#)
- [Suppression de la politique de compartiment pour votre compartiment Amazon S3 on Outposts.](#)
- [Exemples de politique de compartiment](#)

Ajout ou modification d'une politique de compartiment pour un compartiment Amazon S3 on Outposts.

Une politique de compartiment est une politique basée sur les ressources Gestion des identités et des accès AWS (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. Pour de plus amples informations, veuillez consulter [Politique de compartiment](#).

Les rubriques suivantes vous montrent comment mettre à jour votre politique de compartiment Amazon S3 on Outposts en utilisant le AWS Management Console, AWS Command Line Interface (AWS CLI) ou. AWS SDK pour Java

Utilisation de la console S3

Pour créer ou modifier une stratégie 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 Outposts buckets (Compartiments Outposts).
3. Sélectionnez le compartiment Outpost dont vous souhaitez modifier la politique de compartiment.
4. Sélectionnez l'onglet Autorisations.
5. Dans la section Outposts bucket policy (Politique de compartiment des Outposts), pour créer ou modifier une nouvelle politique, sélectionnez Edit (Modifier).

Vous pouvez maintenant ajouter ou modifier la stratégie de compartiment S3 on Outposts. Pour de plus amples informations, veuillez consulter [Configuration d'IAM avec S3 sur Outposts](#).

En utilisant le AWS CLI

L' AWS CLI exemple suivant place une politique dans un bucket Outposts.

1. Enregistrez la stratégie de compartiment suivante dans un fichier JSON. Dans cet exemple, le fichier est nommé `policy1.json`. Remplacez *user input placeholders* par vos propres informations.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "testBucketPolicy",
  "Statement": [
    {
      "Sid": "st1",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:root"
      },
      "Action": [
        "s3-outposts:GetObject",
        "s3-outposts:PutObject",
        "s3-outposts>DeleteObject",
        "s3-outposts:ListBucket"
      ],
      "Resource": "arn:aws:s3-outposts:us-east-1:123456789012:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket"
    }
  ]
}
```

2. Envoyez le fichier JSON en tant que partie de la commande CLI `put-bucket-policy`. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control put-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket --policy file://policy1.json
```

Utilisation du AWS SDK pour Java

L'exemple d'utilisation du kit SDK pour Java suivant place une stratégie sur un compartiment Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void putBucketPolicy(String bucketArn) {

    String policy = "{\"Version\":\"2012-10-17\",\"Id\":\"testBucketPolicy\",
\"Statement\":[[{\"Sid\":\"st1\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"" +
    AccountId+ "\"},\"Action\":\"s3-outposts:*\",\"Resource\":\"" + bucketArn + "\"}]]}";

    PutBucketPolicyRequest reqPutBucketPolicy = new PutBucketPolicyRequest()
        .withAccountId(AccountId)
        .withBucket(bucketArn)
        .withPolicy(policy);

    PutBucketPolicyResult respPutBucketPolicy =
s3ControlClient.putBucketPolicy(reqPutBucketPolicy);
    System.out.printf("PutBucketPolicy Response: %s%n",
respPutBucketPolicy.toString());
}
```

Affichage de la politique de compartiment pour votre compartiment Amazon S3 on Outposts.

Une politique de compartiment est une politique de Gestion des identités et des accès AWS (IAM) basée sur les ressources 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. Pour de plus amples informations, consultez [Politique de compartiment](#).

Les rubriques suivantes vous montrent comment afficher votre stratégie de compartiment Amazon S3 on Outposts à l'aide d'AWS Management Console, d'AWS Command Line Interface (AWS CLI), ou du kit AWS SDK pour Java.

Utilisation de la console S3

Pour créer ou modifier une stratégie de compartiment

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts dont vous souhaitez modifier l'autorisation.
4. Choisissez l'onglet Autorisations.
5. Dans la section Outposts bucket policy (Politique de compartiment des Outposts), vous pouvez passer en revue votre politique de compartiment existante. Pour de plus amples informations, consultez [Configuration d'IAM avec S3 sur Outposts](#).

Utilisation de la AWS CLI

L'exemple suivant d'utilisation de la AWS CLI obtient une stratégie pour un compartiment Outposts. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket
```

Utilisation du kit AWS SDK pour Java

L'exemple de kit SDK pour Java suivant illustre l'obtention d'une stratégie sur un compartiment Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void getBucketPolicy(String bucketArn) {

    GetBucketPolicyRequest reqGetBucketPolicy = new GetBucketPolicyRequest()
        .withAccountId(AccountId)
        .withBucket(bucketArn);

    GetBucketPolicyResult respGetBucketPolicy =
        s3ControlClient.getBucketPolicy(reqGetBucketPolicy);
}
```

```
System.out.printf("GetBucketPolicy Response: %s%n",
respGetBucketPolicy.toString());
}
```

Suppression de la politique de compartiment pour votre compartiment Amazon S3 on Outposts.

Une politique de compartiment est une politique de Gestion des identités et des accès AWS (IAM) basée sur les ressources 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. Pour de plus amples informations, consultez [Politique de compartiment](#).

Les rubriques suivantes vous montrent comment afficher votre stratégie de compartiment Amazon S3 on Outposts à l'aide d'AWS Management Console ou d'AWS Command Line Interface (AWS CLI).

Utilisation de la console S3

Pour supprimer une stratégie de compartiment

1. Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts dont vous souhaitez modifier l'autorisation.
4. Choisissez l'onglet Autorisations.
5. Dans la section Outposts bucket policy (Stratégie de compartiment Outposts), sélectionnez Delete (Supprimer).
6. Confirmez la suppression.

Utilisation de l'AWS CLI

L'exemple suivant supprime la stratégie de compartiment pour un compartiment S3 on Outposts (`s3-outposts:DeleteBucket`) en utilisant AWS CLI. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control delete-bucket-policy --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket
```

Exemples de politique de compartiment

Grâce aux politiques de compartiments S3 sur Outposts, vous pouvez sécuriser l'accès aux objets de vos compartiments S3 sur Outposts, 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 S3 sur Outposts.

Cette section présente des exemples de cas d'utilisation standard de politiques de compartiments S3 sur Outposts. 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 donnée, comme `.html`.

Pour plus d'informations sur le langage de politique Gestion des identités et des accès AWS (IAM), consultez [Configuration d'IAM avec S3 sur Outposts](#).

Note

Lors du test des autorisations [s3outposts](#) à l'aide de la console Amazon S3, vous devez accorder les autorisations supplémentaires requises par la console, telles que `s3outposts:createendpoint`, `s3outposts:listendpoints`, etc.

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 S3 sur Outposts, consultez [Actions, ressources et clés de condition pour Amazon S3 sur Outposts](#).
- Pour obtenir des conseils sur la création de votre politique S3 sur Outposts, consultez [Ajout ou modification d'une politique de compartiment pour un compartiment Amazon S3 on Outposts..](#)

Rubriques

- [Gestion de l'accès à un compartiment Amazon S3 sur Outposts en fonction d'adresses IP spécifiques](#)

Gestion de l'accès à un compartiment Amazon S3 sur Outposts en fonction d'adresses IP spécifiques

Une politique de compartiment est une politique basée sur les ressources Gestion des identités et des accès AWS (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. Pour de plus amples informations, veuillez consulter [Politique de compartiment](#).

Restriction de l'accès à des adresses IP spécifiques

L'exemple suivant interdit à tous les utilisateurs d'effectuer des [opérations S3 sur Outposts](#) sur les objets des compartiments spécifiés, sauf si la demande provient de la plage d'adresses IP spécifiée.

Note

Lorsque vous limitez l'accès à une adresse IP spécifique, veillez à spécifier également les points de terminaison de VPC, les adresses IP sources de VPC ou les adresses IP externes qui peuvent accéder au compartiment S3 sur Outposts. Dans le cas contraire, vous risquez de perdre l'accès au compartiment si votre politique interdit à tous les utilisateurs d'effectuer des opérations [s3outposts](#) sur les objets de votre compartiment S3 sur Outposts sans que les autorisations appropriées ne soient déjà en place.

La Condition déclaration de cette politique s'identifie **192.0.2.0/24** comme la plage d'adresses IP autorisées version 4 (IPv4).

Le Condition bloc utilise la NotIpAddress condition et la clé de `aws:SourceIp` condition, qui est une clé AWS de condition large. La clé de condition `aws:SourceIp` ne peut être utilisée que pour les plages d'adresses IP publiques. Pour plus d'informations sur ces clés de condition, consultez [Actions, ressources et clés de condition pour S3 sur Outposts](#). Les `aws:SourceIp` IPv4 valeurs

utilisent la notation CIDR standard. Pour plus d'informations, consultez [Références des éléments de politique JSON IAM](#) dans le Guide de l'utilisateur IAM.

⚠ Warning

Avant d'employer cette politique S3 sur Outposts, remplacez la plage d'adresses IP **192.0.2.0/24** de cet exemple par une valeur appropriée pour votre cas d'utilisation. Dans le cas contraire, vous perdrez la possibilité d'accéder à votre compartiment.

```
{
  "Version": "2012-10-17",
  "Id": "S3OutpostsPolicyId1",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Deny",
      "Principal": "*",
      "Action": "s3-outposts:*",
      "Resource": [
        "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
accesspoint/EXAMPLE-ACCESS-POINT-NAME",
        "arn:aws:aws:s3-outposts:region:111122223333:outpost/OUTPOSTS-ID/
bucket/amzn-s3-demo-bucket"
      ],
      "Condition": {
        "NotIpAddress": {
          "aws:SourceIp": "192.0.2.0/24"
        }
      }
    }
  ]
}
```

Autoriser à la fois IPv4 et IPv6 les adresses

Lorsque vous commencez à utiliser IPv6 des adresses, nous vous recommandons de mettre à jour toutes les politiques de votre organisation avec vos plages d' IPv6 adresses en plus de vos IPv4 plages existantes. Cela vous aidera à faire en sorte que les politiques continuent de fonctionner pendant la transition vers IPv6.

L'exemple de politique de compartiment S3 on Outposts suivant montre comment combiner des plages IPv4 d' IPv6 adresses pour couvrir toutes les adresses IP valides de votre organisation. Dans cet exemple, la politique autorise l'accès aux exemples d'adresses IP **192.0.2.1** et **2001:DB8:1234:5678::1** et le refuse aux adresses **203.0.113.1** et **2001:DB8:1234:5678:ABCD::1**.

La clé de condition `aws:SourceIp` ne peut être utilisée que pour les plages d'adresses IP publiques. Les IPv6 valeurs pour `aws:SourceIp` doivent être au format CIDR standard. En IPv6 effet, nous prenons en charge l'utilisation `::` pour représenter une plage de 0 (par exemple, `2001:DB8:1234:5678::/64`). Pour plus d'informations, consultez [Opérateurs de condition d'adresse IP](#) dans le guide de l'utilisateur IAM.

Warning

Remplacez les plages d'adresses IP de cet exemple par des valeurs appropriées pour votre cas d'utilisation avant d'employer cette politique S3 sur Outposts. Dans le cas contraire, vous pourriez perdre la possibilité d'accéder à votre compartiment.

JSON

```
{
  "Id": "S3OutpostsPolicyId2",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIPmix",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": [
        "s3-outposts:GetObject",
        "s3-outposts:PutObject",
        "s3-outposts:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3-outposts:us-east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket",
```

```
    "arn:aws:s3-outposts:us-  
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket/*"  
  ],  
  "Condition": {  
    "IpAddress": {  
      "aws:SourceIp": [  
        "192.0.2.0/24",  
        "2001:DB8:1234:5678::/64"  
      ]  
    },  
    "NotIpAddress": {  
      "aws:SourceIp": [  
        "203.0.113.0/24",  
        "2001:DB8:1234:5678:ABCD::/80"  
      ]  
    }  
  }  
}  
]  
}
```

Lister les compartiments Amazon S3 on Outposts

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur APIs les compartiments Outpost que sur les compartiments 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 Command Line Interface (AWS CLI) ou REST. AWS SDKs Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Pour plus d'informations sur l'utilisation des compartiments dans S3 on Outposts, voir [Utilisation des compartiments S3 on Outposts](#).

Les exemples suivants vous montrent comment renvoyer une liste de vos compartiments S3 sur Outposts en utilisant les touches AWS Management Console, et AWS CLI. AWS SDK pour Java

Utilisation de la console S3

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Sous Outposts buckets (Compartiments Outposts), vérifiez votre liste de compartiments S3 on Outposts.

À l'aide du AWS CLI

L' AWS CLI exemple suivant permet d'obtenir une liste de buckets dans un Outpost. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour plus d'informations sur cette commande, reportez-vous [list-regional-buckets](#) à la section AWS CLI Référence.

```
aws s3control list-regional-buckets --account-id 123456789012 --outpost-id op-01ac5d28a6a232904
```

Utilisation du AWS SDK pour Java

L'exemple de kit SDK pour Java suivant illustre l'obtention d'une liste de compartiments dans un Outpost. Pour plus d'informations, consultez [ListRegionalBuckets](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void listRegionalBuckets() {

    ListRegionalBucketsRequest reqListBuckets = new ListRegionalBucketsRequest()
        .withAccountId(AccountId)
        .withOutpostId(OutpostId);

    ListRegionalBucketsResult respListBuckets =
s3ControlClient.listRegionalBuckets(reqListBuckets);
    System.out.printf("ListRegionalBuckets Response: %s%n",
respListBuckets.toString());
}
```

}

Obtenir un bucket S3 on Outposts à l'aide du SDK AWS CLI et du SDK pour Java

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur APIs les compartiments Outpost que sur les compartiments 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 Command Line Interface (AWS CLI) ou REST. AWS SDKs Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Les exemples suivants vous montrent comment obtenir un bucket S3 on Outposts en utilisant le AWS CLI et. AWS SDK pour Java

Note

Lorsque vous travaillez avec Amazon S3 sur des Outposts via le AWS CLI ou AWS SDKs, vous fournissez l'ARN du point d'accès pour l'Outpost à la place du nom du bucket. L'ARN du point d'accès prend la forme suivante, où *region* est le code Région AWS pour la région où l'Outpost est situé :

```
arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/  
accesspoint/example-outposts-access-point
```

Pour plus d'informations sur S3 on Outposts ARNs, consultez. [Ressource ARNs pour S3 sur les Outposts](#)

À l'aide du AWS CLI

L'exemple S3 on Outposts suivant obtient un compartiment à l'aide de l' AWS CLI. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour de

plus amples informations sur cette commande, veuillez consulter [get-bucket](#) dans le document AWS CLI Reference.

```
aws s3control get-bucket --account-id 123456789012 --bucket "arn:aws:s3-  
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-  
bucket"
```

Utilisation du AWS SDK pour Java

L'exemple S3 on Outposts suivant illustre l'obtention d'un compartiment à l'aide du kit SDK pour Java. Pour plus d'informations, consultez [GetBucket](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;  
  
public void getBucket(String bucketArn) {  
  
    GetBucketRequest reqGetBucket = new GetBucketRequest()  
        .withBucket(bucketArn)  
        .withAccountId(AccountId);  
  
    GetBucketResult respGetBucket = s3ControlClient.getBucket(reqGetBucket);  
    System.out.printf("GetBucket Response: %s%n", respGetBucket.toString());  
  
}
```

Suppression de votre compartiment Amazon S3 on Outposts

Avec Amazon S3 sur Outposts, vous pouvez créer des compartiments S3 sur votre AWS Outposts afin de stocker et récupérer facilement des objets sur site pour des applications qui nécessitent un accès aux données locales, un traitement local des données et une résidence des données. S3 sur Outposts propose une nouvelle classe de stockage, appelée S3 Outposts (OUTPOSTS), qui utilise les API Amazon S3 et est conçue pour stocker de manière durable et redondante des données sur plusieurs appareils et serveurs sur vos AWS Outposts. Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes API et fonctions sur vos compartiments Outpost que sur les compartiments Amazon S3, telles que les stratégies d'accès, le chiffrement et le balisage. Vous pouvez utiliser S3 sur Outposts via la AWS Management Console, l'AWS Command Line

Interface (AWS CLI), des kits SDK AWS ou une API REST. Pour de plus amples informations, veuillez consulter [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Pour plus d'informations sur l'utilisation des compartiments dans S3 on Outposts, voir [Utilisation des compartiments S3 on Outposts](#).

Le compte Compte AWS qui crée le compartiment en est le propriétaire, et lui seul le supprimer.

Note

- Les compartiments Outposts doivent être vides avant de pouvoir être supprimés.

La console Amazon S3 ne prend pas en charge les actions sur les objets S3 on Outposts. Pour supprimer des objets dans un compartiment S3 on Outposts, vous devez utiliser l'API REST, AWS CLI ou les kits SDK AWS.

- Pour pouvoir supprimer un compartiment Outposts, vous devez supprimer tous les points d'accès Outposts pour le compartiment. Pour de plus amples informations, consultez [Suppression d'un point d'accès](#).
- Vous ne pouvez pas récupérer un compartiment après l'avoir supprimé.

Les exemples suivants vous montrent comment supprimer un compartiment S3 on Outposts à l'aide d'AWS Management Console et d'AWS Command Line Interface (AWS CLI).

Utilisation de la console S3

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment à supprimer, puis choisissez Delete (Supprimer).
4. Confirmez la suppression.

Utilisation de l'AWS CLI

L'exemple suivant supprime un compartiment S3 on Outposts (`s3-outposts:DeleteBucket`) à l'aide d'AWS CLI. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control delete-bucket --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket
```

Utilisation des points d'accès Amazon S3 on Outposts

Pour accéder à votre compartiment Amazon S3 on Outposts, vous devez créer et configurer un point 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 points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet Amazon S3, notamment `GetObject` et `PutObject`. Avec S3 on Outposts, vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outposts. Les points d'accès prennent uniquement en charge l'adressage de type hôte virtuel.

Note

Le compte Compte AWS qui crée le compartiment Outposts en est le propriétaire, et lui seul peut lui attribuer des points d'accès.

Les sections suivantes décrivent comment créer et gérer des points d'accès pour les compartiments S3 on Outposts.

Rubriques

- [Création d'un point d'accès S3 on Outposts](#)
- [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#)
- [Affichage d'informations sur la configuration d'un point d'accès](#)
- [Afficher une liste de vos points d'accès Amazon S3 on Outposts](#)

- [Suppression d'un point d'accès](#)
- [Ajout ou modification d'une stratégie de point d'accès](#)
- [Affichage d'une stratégie d'accès pour un point d'accès S3 on Outposts.](#)

Création d'un point d'accès S3 on Outposts

Pour accéder à votre compartiment Amazon S3 sur Outposts, vous devez créer et configurer un point 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 points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet Amazon S3, notamment `GetObject` et `PutObject`. Avec S3 on Outposts, vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outposts. Les points d'accès prennent uniquement en charge l'adressage de type hôte virtuel.

Les exemples suivants vous montrent comment créer un point d'accès S3 on Outposts à l'aide d'AWS Management Console, d'AWS Command Line Interface (AWS CLI) et du kit AWS SDK pour Java.

Note

Le compte Compte AWS qui crée le compartiment Outposts en est le propriétaire, et lui seul peut lui attribuer des points d'accès.

Utilisation de la console S3

1. Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts pour lequel vous souhaitez créer un point d'accès Outposts.
4. Sélectionnez l'onglet Outposts access points (Points d'accès Outposts).
5. Dans la section Outposts access points (Points d'accès Outposts), choisissez Create Outposts access point (Créer un point d'accès Outposts).

6. Dans Outposts access point settings (Paramètres du point d'accès Outposts), attribuez un nom au point d'accès, puis choisissez le cloud privé virtuel (VPC) du point d'accès.
7. Si vous voulez ajouter une stratégie pour votre point d'accès, saisissez-la dans la section Outposts access point policy (Stratégie de point d'accès Outposts).

Pour plus d'informations, consultez [Configuration d'IAM avec S3 sur Outposts](#).

Utilisation de la AWS CLI

Exemple

L'exemple AWS CLI suivant crée un point d'accès pour un compartiment Outposts. Pour exécuter cette commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3control create-access-point --account-id 123456789012
--name example-outposts-access-point --bucket "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket" --vpc-configuration VpcId=example-vpc-12345
```

Utilisation du kit AWS SDK pour Java

Exemple

Pour des exemples de création d'un point d'accès pour un compartiment S3 Outposts avec le kit AWS SDK pour Java, consultez [CreateOutpostsAccessPoint.java](#) dans les Exemples de code du kit AWS SDK pour Java 2.x.

Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts

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. Par exemple, vous pouvez utiliser un alias de point d'accès pour effectuer des opérations au niveau de l'objet telles que PUT, GET, LIST, etc. Pour obtenir la liste de ces opérations, consultez la page [Opérations d'API Amazon S3 pour la gestion des objets](#).

Voici des exemples d'ARN et d'alias de point d'accès pour un point d'accès nommé *my-access-point*.

- ARN du point d'accès – `arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/my-access-point`
- Alias de point d'accès – `my-access-po-001ac5d28a6a232904e8xz5w8ijx1qzlb3i3kuse10--op-s3`

Pour plus d'informations sur ARNs, consultez [Amazon Resource Names \(ARNs\)](#) dans le Références générales AWS.

Pour plus d'informations sur les alias de point d'accès, consultez les rubriques suivantes.

Rubriques

- [Alias de point d'accès](#)
- [Utilisation d'un alias de point d'accès dans une opération d'objet S3 sur Outposts](#)
- [Limites](#)

Alias de point d'accès

Un alias de point d'accès est créé dans le même espace de noms qu'un compartiment S3 sur Outposts. Lorsque vous créez un point d'accès, S3 sur Outposts génère automatiquement un alias de point d'accès qui ne peut pas être modifié. Un alias de point d'accès répond à toutes les exigences d'un nom de compartiment S3 sur Outposts valide et comprend les parties suivantes :

access point name prefix-metadata--op-s3

Note

Le suffixe `--op-s3` est réservé aux alias de point d'accès. Nous vous recommandons de ne pas l'utiliser pour les noms de compartiment ou de point d'accès. Pour plus d'informations sur les règles d'attribution de noms des compartiments S3 sur Outposts, consultez [Utilisation des compartiments S3 on Outposts](#).

Recherche de l'alias de point d'accès

Les exemples suivants vous montrent comment trouver un alias de point d'accès à l'aide de la console Amazon S3 et de l'interface AWS CLI.

Exemple: Rechercher et copier l'alias d'un point d'accès dans la console Amazon S3

Après avoir créé un point d'accès dans la console, vous pouvez obtenir l'alias de point d'accès dans la colonne Access Point alias (Alias de point d'accès) de la liste Access Points (Points d'accès).

Copier l'alias 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 de gauche, choisissez Points d'accès Outposts.
3. Pour copier l'alias de point d'accès, effectuez l'une des opérations suivantes :
 - Dans la liste des Access Points (Points d'accès), sélectionnez le bouton d'option à côté du nom du point d'accès, puis choisissez Copy Access Point alias (Copier un alias de point d'accès).
 - Choisissez le nom du point d'accès. Ensuite, sous Outposts access point overview (Présentation du point d'accès Outposts), copiez l'alias de point d'accès.

Exemple: créez un point d'accès en utilisant AWS CLI et recherchez l'alias du point d'accès dans la réponse

L' AWS CLI exemple de `create-access-point` commande suivant crée le point d'accès et renvoie l'alias du point d'accès généré automatiquement. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control create-access-point --bucket example-outposts-bucket --name example-outposts-access-point --account-id 123456789012

{
  "AccessPointArn":
    "arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/
    accesspoint/example-outposts-access-point",
  "Alias": "example-outp-o01ac5d28a6a232904e8xz5w8ijx1qz1bp3i3kuse10--op-s3"
}
```

Exemple: obtenez un alias de point d'accès à l'aide du AWS CLI

L' AWS CLI exemple de `get-access-point` commande suivant renvoie des informations sur le point d'accès spécifié. Ces informations incluent l'alias de point d'accès. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-access-point --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket --name example-outposts-access-point --account-id 123456789012

{
  "Name": "example-outposts-access-point",
  "Bucket": "example-outposts-bucket",
  "NetworkOrigin": "Vpc",
  "VpcConfiguration": {
    "VpcId": "vpc-01234567890abcdef"
  },
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": true,
    "IgnorePublicAcls": true,
    "BlockPublicPolicy": true,
    "RestrictPublicBuckets": true
  },
  "CreationDate": "2022-09-18T17:49:15.584000+00:00",
  "Alias": "example-outp-o0b1d075431d83bebde8xz5w8ijx1qz1bp3i3kuse10--op-s3"
}
```

Exemple: Répertoriez les points d'accès pour trouver un alias de point d'accès à l'aide du AWS CLI

L' AWS CLI exemple de `list-access-points` commande suivant répertorie les informations relatives au point d'accès spécifié. Ces informations incluent l'alias de point d'accès. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control list-access-points --account-id 123456789012 --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-
bucket

{
  "AccessPointList": [
    {
      "Name": "example-outposts-access-point",
      "NetworkOrigin": "Vpc",
      "VpcConfiguration": {
        "VpcId": "vpc-01234567890abcdef"
      },
      "Bucket": "example-outposts-bucket",
      "AccessPointArn": "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-
access-point",
```

```
        "Alias": "example-utp-o0b1d075431d83bebde8xz5w8ijx1qzlp3i3kuse10--op-s3"
    }
}
}
```

Utilisation d'un alias de point d'accès dans une opération d'objet S3 sur Outposts

Lorsque vous adoptez des points d'accès, vous pouvez utiliser des alias de point d'accès sans nécessiter d'importantes modifications du code.

Cet AWS CLI exemple montre une `get-object` opération pour un bucket S3 on Outposts. Cet exemple utilise l'alias de point d'accès comme valeur pour `--bucket` au lieu de l'ARN complet du point d'accès.

```
aws s3api get-object --bucket my-access-po-
o0b1d075431d83bebde8xz5w8ijx1qzlp3i3kuse10--op-s3 --key testkey sample-object.rtf

{
  "AcceptRanges": "bytes",
  "LastModified": "2020-01-08T22:16:28+00:00",
  "ContentLength": 910,
  "ETag": "\"00751974dc146b76404bb7290f8f51bb\"",
  "VersionId": "null",
  "ContentType": "text/rtf",
  "Metadata": {}
}
```

Limites

- 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 ne pouvez pas utiliser un alias de point d'accès pour les opérations relatives au plan de contrôle S3 sur Outposts. Pour une liste des opérations du plan de contrôle S3 sur Outposts, consultez [Opérations d'API de contrôle Amazon S3 pour la gestion des compartiments](#).
- Les alias ne peuvent pas être utilisés dans les Gestion des identités et des accès AWS politiques (IAM).

Affichage d'informations sur la configuration d'un point 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 points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet Amazon S3, notamment `GetObject` et `PutObject`. Avec S3 on Outposts, vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outposts. Les points d'accès ne prennent en charge que l' virtual-host-styleadressage.

Les rubriques suivantes expliquent comment renvoyer des informations de configuration pour un point d'accès S3 on Outposts à l'aide des touches AWS Management Console, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java

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 Points d'accès Outposts.
3. Sélectionnez le point d'accès Outpost pour lequel vous souhaitez afficher les détails de la configuration.
4. Sous Outposts access point overview (Aperçu du point d'accès Outpost), passez en revue les détails de la configuration du point d'accès.

À l'aide du AWS CLI

L' AWS CLI exemple suivant permet d'obtenir un point d'accès pour un bucket Outposts. Remplacez les *user input placeholders* par vos propres informations.

```
aws s3control get-access-point --account-id 123456789012 --name arn:aws:s3-  
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-  
access-point
```

Utilisation du AWS SDK pour Java

L'exemple de kit SDK pour Java suivant illustre l'obtention d'un point d'accès pour un compartiment Outposts.

```
import com.amazonaws.services.s3control.model.*;
```

```
public void getAccessPoint(String accessPointArn) {  
  
    GetAccessPointRequest reqGetAP = new GetAccessPointRequest()  
        .withAccountId(AccountId)  
        .withName(accessPointArn);  
  
    GetAccessPointResult respGetAP = s3ControlClient.getAccessPoint(reqGetAP);  
    System.out.printf("GetAccessPoint Response: %s%n", respGetAP.toString());  
  
}
```

Afficher une liste de vos points d'accès Amazon S3 on Outposts

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 points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet Amazon S3, notamment `GetObject` et `PutObject`. Avec S3 on Outposts, vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outposts. Les points d'accès ne prennent en charge que l' virtual-host-styleadressage.

Les rubriques suivantes vous montrent comment renvoyer une liste de vos points d'accès S3 sur Outposts à l'aide des touches AWS Management Console, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java

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 Points d'accès Outposts.
3. Sous Outposts access points (Points d'accès aux Outposts), passez en revue votre liste de points d'accès S3 on Outposts.

À l'aide du AWS CLI

L' AWS CLI exemple suivant répertorie les points d'accès pour un bucket Outposts. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control list-access-points --account-id 123456789012 --bucket arn:aws:s3-  
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-  
bucket
```

Utilisation du AWS SDK pour Java

L'exemple de kit SDK pour Java suivant répertorie les points d'accès pour un compartiment Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void listAccessPoints(String bucketArn) {

    ListAccessPointsRequest reqListAPs = new ListAccessPointsRequest()
        .withAccountId(AccountId)
        .withBucket(bucketArn);

    ListAccessPointsResult respListAPs = s3ControlClient.listAccessPoints(reqListAPs);
    System.out.printf("ListAccessPoints Response: %s%n", respListAPs.toString());
}
```

Suppression d'un point 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 points de terminaison réseau associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet Amazon S3, notamment `GetObject` et `PutObject`. Avec S3 on Outposts, vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outposts. Les points d'accès prennent uniquement en charge l'adressage de type hôte virtuel.

Les exemples suivants vous montrent comment supprimer un point d'accès à l'aide d'AWS Management Console et d'AWS Command Line Interface (AWS CLI).

Utilisation de la console S3

1. Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts access points (Points d'accès Outposts).
3. Dans la section Outposts access points (Points d'accès Outposts), choisissez le point d'accès Outposts à supprimer.
4. Sélectionnez Delete.
5. Confirmez la suppression.

Utilisation de l'AWS CLI

L'exemple AWS CLI suivant supprime un point d'accès Outposts. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control delete-access-point --account-id 123456789012 --name arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-access-point
```

Ajout ou modification d'une stratégie de point d'accès

Les points d'accès disposent d'autorisations et de contrôles de réseau distincts qu'Amazon S3 on Outposts applique pour toute requête effectuée via ce point d'accès. 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, consultez [Points d'accès](#).

Les rubriques suivantes vous montrent comment ajouter ou modifier la stratégie de votre point d'accès S3 on Outposts à l'aide d'AWS Management Console, d'AWS Command Line Interface (AWS CLI) et d'AWS SDK pour Java.

Utilisation de la console S3

1. Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts pour lequel vous souhaitez modifier la stratégie de point d'accès.
4. Sélectionnez l'onglet Outposts access points (Points d'accès Outposts).
5. Dans la section Outposts access points (Points d'accès Outposts), sélectionnez le point d'accès dont vous voulez modifier la stratégie, puis Edit policy (Modifier la stratégie).
6. Ajoutez ou modifiez la stratégie dans la section Outposts access point policy (Stratégie de point d'accès Outposts). Pour de plus amples informations, consultez [Configuration d'IAM avec S3 sur Outposts](#).

Utilisation de la AWS CLI

L'exemple d'utilisation de la AWS CLI suivant place une stratégie sur un point d'accès Outposts.

1. Enregistrez la stratégie de point d'accès suivante dans un fichier JSON. Dans cet exemple, le fichier est nommé `appolicy1.json`. Remplacez *user input placeholders* par vos propres informations.

```
{
  "Version":"2012-10-17",
  "Id":"exampleAccessPointPolicy",
  "Statement":[
    {
      "Sid":"st1",
      "Effect":"Allow",
      "Principal":{
        "AWS":"123456789012"
      },
      "Action":"s3-outposts:*",
      "Resource":"arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point
    }
  ]
}
```

2. Envoyez le fichier JSON en tant que partie de la commande CLI `put-access-point-policy`. Remplacez *user input placeholders* par vos propres informations.

```
aws s3control put-access-point-policy --account-id 123456789012 --name arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --policy file://appolicy1.json
```

Utilisation du kit AWS SDK pour Java

L'exemple suivant d'utilisation du kits SDK pour Java place une stratégie sur un point d'accès Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void putAccessPointPolicy(String accessPointArn) {

    String policy = "{\"Version\":\"2012-10-17\",\"Id\":\"testAccessPointPolicy\",
\"Statement\": [{\"Sid\":\"st1\",\"Effect\":\"Allow\",\"Principal\":{\"AWS\":\"" +
```

```
AccountId + "\",\"Action\": \"s3-outposts:*\", \"Resource\": \"" + accessPointArn +
"\"]}]";

PutAccessPointPolicyRequest reqPutAccessPointPolicy = new
PutAccessPointPolicyRequest()
    .withAccountId(AccountId)
    .withName(accessPointArn)
    .withPolicy(policy);

PutAccessPointPolicyResult respPutAccessPointPolicy =
s3ControlClient.putAccessPointPolicy(reqPutAccessPointPolicy);
System.out.printf("PutAccessPointPolicy Response: %s%n",
respPutAccessPointPolicy.toString());
    printWriter.printf("PutAccessPointPolicy Response: %s%n",
respPutAccessPointPolicy.toString());
}
```

Affichage d'une stratégie d'accès pour un point d'accès S3 on Outposts.

Les points d'accès disposent d'autorisations et de contrôles de réseau distincts qu'Amazon S3 on Outposts applique pour toute requête effectuée via ce point d'accès. 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, consultez [Points d'accès](#).

Pour plus d'informations sur l'utilisation des points d'accès dans S3 on Outposts, voir [Utilisation des compartiments S3 on Outposts](#).

Les rubriques suivantes vous montrent comment afficher votre stratégie de point d'accès S3 on Outposts à l'aide d'AWS Management Console, d'AWS Command Line Interface (AWS CLI) et du kit AWS SDK pour Java.

Utilisation de la console S3

1. Ouvrez la console Amazon S3 sur <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts access points (Points d'accès Outposts).
3. Sélectionnez le point d'accès Outpost pour lequel vous souhaitez afficher la stratégie.
4. Dans la page Permissions (Autorisations), consultez la stratégie de point d'accès S3 on Outposts.

5. Pour modifier une stratégie de point d'accès, voir [Ajout ou modification d'une stratégie de point d'accès](#).

Utilisation de l'AWS CLI

L'exemple d'utilisation de la AWS CLI suivant obtient une stratégie pour un point d'accès Outposts. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control get-access-point-policy --account-id 123456789012 --name arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-access-point
```

Utilisation du kit AWS SDK pour Java

L'exemple d'utilisation du kit SDK pour Java suivant obtient une stratégie pour un point d'accès Outposts.

```
import com.amazonaws.services.s3control.model.*;

public void getAccessPointPolicy(String accessPointArn) {

    GetAccessPointPolicyRequest reqGetAccessPointPolicy = new
    GetAccessPointPolicyRequest()
        .withAccountId(AccountId)
        .withName(accessPointArn);

    GetAccessPointPolicyResult respGetAccessPointPolicy =
    s3ControlClient.getAccessPointPolicy(reqGetAccessPointPolicy);
    System.out.printf("GetAccessPointPolicy Response: %s%n",
    respGetAccessPointPolicy.toString());
    printWriter.printf("GetAccessPointPolicy Response: %s%n",
    respGetAccessPointPolicy.toString());

}
```

Utilisation des points de terminaison Amazon S3 sur Outposts

Pour acheminer les demandes vers un point d'accès Amazon S3 sur Outposts, vous devez créer et configurer un point de terminaison S3 sur Outposts. Pour créer un point de terminaison, vous

devrez disposer d'une connexion active avec votre lien de service vers votre région d'accueil Outpost. Chaque cloud privé virtuel (VPC) sur votre Outpost peut avoir un point de terminaison associé. Pour plus d'informations sur les quotas de points de terminaison, consultez [Exigences réseau de S3 on Outposts](#). Vous devez créer un point de terminaison pour pouvoir accéder à vos compartiments Outpost et effectuer des opérations d'objet. Pour de plus amples informations, consultez [Points de terminaison](#).

Après avoir créé un point de terminaison, vous pouvez utiliser le champ « Statut » pour comprendre l'état du point de terminaison. Si votre Outpost est hors ligne, il renverra CREATE_FAILED.

Vous pouvez vérifier la connexion de votre lien de service, supprimer le point de terminaison et recommencer l'opération de création une fois la connexion rétablie. Vous pouvez consulter une liste des codes d'erreur supplémentaires ci-dessous. Pour de plus amples informations, consultez [Points de terminaison](#).

« Hello, World! »	Statut	Code d'erreur du motif de l'échec	Message – Motif de l'échec
CreateEndpoint	Create_Failed	OutpostNotReachable	Le point de terminaison n'a pas pu être créé car la connexion du lien de service vers votre région d'accueil Outpost est interrompue. Vérifiez votre connexion, supprimez le point de terminaison et réessayez.
CreateEndpoint	Create_Failed	InternalServerError	Le point de terminaison n'a pas pu être créé en raison d'une erreur interne. Veuillez supprimer le point de terminaison et le créer à nouveau.
DeleteEndpoint	Échec de la suppression	OutpostNotReachable	Le point de terminaison n'a pas pu être supprimé car la connexion du lien de service vers votre région d'accueil Outpost est interrompue. Vérifiez votre connexion et réessayez.
DeleteEndpoint	Échec de la	InternalServerError	Le point de terminaison n'a pas pu être supprimé en raison d'une erreur interne. Veuillez réessayer.

« Hello, World! »	Statut	Code d'erreur du motif de l'échec	Message – Motif de l'échec
	suppression		

Pour de plus amples informations sur l'utilisation des compartiments dans S3 on Outposts, veuillez consulter [Utilisation des compartiments S3 on Outposts](#).

Les sections suivantes décrivent comment créer et gérer des points de terminaison pour S3 on Outposts.

Rubriques

- [Création d'un point de terminaison sur un Outpost](#)
- [Affichage d'une liste de vos points de terminaison Amazon S3 on Outposts](#)
- [Suppression d'un point de terminaison Amazon S3 on Outposts](#)

Création d'un point de terminaison sur un Outpost

Pour acheminer les demandes vers un point d'accès Amazon S3 sur Outposts, vous devez créer et configurer un point de terminaison S3 sur Outposts. Pour créer un point de terminaison, vous devrez disposer d'une connexion active avec votre lien de service vers votre région d'accueil Outpost. Chaque cloud privé virtuel (VPC) sur votre Outpost peut avoir un point de terminaison associé. Pour plus d'informations sur les quotas de points de terminaison, consultez [Exigences réseau de S3 on Outposts](#). Vous devez créer un point de terminaison pour pouvoir accéder à vos compartiments Outpost et effectuer des opérations d'objet. Pour plus d'informations, consultez [Points de terminaison](#).

Autorisations

Pour plus d'informations sur les autorisations requises pour créer un point de terminaison, consultez [Autorisations pour les points de terminaison S3 sur Outposts](#).

Lorsque vous créez un point de terminaison, S3 sur Outposts crée également un rôle lié à un service dans votre Compte AWS. Pour plus d'informations, consultez [Utilisation de rôles liés à un service pour Amazon S3 sur Outposts](#).

Les exemples suivants vous montrent comment créer un point de terminaison S3 sur Outposts à l'aide de la AWS Management Console, de l'AWS Command Line Interface (AWS CLI) et du AWS SDK pour Java.

Utilisation de la console S3

1. Connectez-vous à la AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation de gauche, choisissez Points d'accès Outposts.
3. Sélectionnez l'onglet Outposts endpoints (Points de terminaison Outposts).
4. Choisissez Create Outposts endpoint (Créer un point de terminaison Outposts).
5. Sous Outpost, sélectionnez l'Outpost sur lequel créer ce point de terminaison.
6. Sous VPC, sélectionnez un VPC qui n'a pas encore de point de terminaison et qui respecte également les règles relatives aux points de terminaison des Outposts.

Un cloud privé virtuel (VPC) vous permet de lancer des ressources AWS dans un réseau virtuel défini par vos soins. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre centre de données et présente l'avantage d'utiliser l'infrastructure évolutive d'AWS.

Si vous n'avez pas de VPC, choisissez Create VPC (Créer un VPC). Pour plus d'informations, consultez [Création de points d'accès restreints à un cloud privé virtuel \(VPC\)](#) dans le Guide de l'utilisateur Amazon S3.

7. Choisissez Create Outposts endpoint (Créer un point de terminaison Outposts).

Utilisation de la AWS CLI

Exemple

L'exemple d'AWS CLI suivant crée un point de terminaison pour un Outpost à l'aide du type d'accès aux ressources VPC. Le VPC est dérivé du sous-réseau. Pour exécuter cette commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id  
subnet-8c7a57c5 --security-group-id sg-ab19e0d1
```

L'exemple AWS CLI suivant crée un point de terminaison pour un Outpost à l'aide du type d'accès au groupe d'adresses IP clients (groupe CoIP). Pour exécuter cette commande, remplacez les *user input placeholders* par vos propres informations.

```
aws s3outposts create-endpoint --outpost-id op-01ac5d28a6a232904 --subnet-id
  subnet-8c7a57c5 --security-group-id sg-ab19e0d1 --access-type CustomerOwnedIp --
customer-owned-ipv4-pool ipv4pool-coip-12345678901234567
```

Utilisation du kit AWS SDK pour Java

Exemple

Pour des exemples de création d'un point de terminaison pour un S3 Outpost avec le kit AWS SDK pour Java, consultez [CreateOutpostsEndPoint.java](#) dans les Exemples de code du kit AWS SDK pour Java 2.x.

Affichage d'une liste de vos points de terminaison Amazon S3 on Outposts

Pour acheminer les demandes vers un point d'accès Amazon S3 sur Outposts, vous devez créer et configurer un point de terminaison S3 sur Outposts. Pour créer un point de terminaison, vous devrez disposer d'une connexion active avec votre lien de service vers votre région d'accueil Outpost. Chaque cloud privé virtuel (VPC) sur votre Outpost peut avoir un point de terminaison associé. Pour plus d'informations sur les quotas de points de terminaison, consultez [Exigences réseau de S3 on Outposts](#). Vous devez créer un point de terminaison pour pouvoir accéder à vos compartiments Outpost et effectuer des opérations d'objet. Pour de plus amples informations, veuillez consulter [Points de terminaison](#).

Les exemples suivants vous montrent comment renvoyer une liste de vos points de terminaison S3 sur Outposts en utilisant les touches AWS Management Console, AWS Command Line Interface (AWS CLI) et AWS SDK pour Java

Utilisation de la console S3

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts access points (Points d'accès Outposts).
3. Sur la page Outposts access points (Points d'accès des Outposts), sélectionnez l'onglet Outposts endpoints (Points de terminaison des Outposts).

4. Sous Outposts endpoints (Points de terminaison Outposts), vous pouvez afficher la liste de vos points de terminaison S3 sur Outposts.

À l'aide du AWS CLI

L'AWS CLI exemple suivant répertorie les points de terminaison des AWS Outposts ressources associées à votre compte. Pour de plus amples informations sur cette commande, consultez [list-endpoints](#) dans le document AWS CLI Reference.

```
aws s3outposts list-endpoints
```

Utilisation du AWS SDK pour Java

L'exemple d'utilisation du kit SDK pour Java suivant génère une liste des points de terminaison pour un Outpost. Pour plus d'informations, consultez [ListEndpoints](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.ListEndpointsRequest;
import com.amazonaws.services.s3outposts.model.ListEndpointsResult;

public void listEndpoints() {
    AmazonS3Outposts s3OutpostsClient = AmazonS3OutpostsClientBuilder
        .standard().build();

    ListEndpointsRequest listEndpointsRequest = new ListEndpointsRequest();
    ListEndpointsResult listEndpointsResult =
s3OutpostsClient.listEndpoints(listEndpointsRequest);
    System.out.println("List endpoints result is " + listEndpointsResult);
}
```

Suppression d'un point de terminaison Amazon S3 on Outposts

Pour acheminer les demandes vers un point d'accès Amazon S3 sur Outposts, vous devez créer et configurer un point de terminaison S3 sur Outposts. Pour créer un point de terminaison, vous devrez disposer d'une connexion active avec votre lien de service vers votre région d'accueil Outpost. Chaque cloud privé virtuel (VPC) sur votre Outpost peut avoir un point de terminaison associé. Pour plus d'informations sur les quotas de points de terminaison, consultez [Exigences réseau de S3 on Outposts](#). Vous devez créer un point de terminaison pour pouvoir accéder à vos compartiments

Outpost et effectuer des opérations d'objet. Pour de plus amples informations, veuillez consulter [Points de terminaison](#).

Les exemples suivants vous montrent comment supprimer votre S3 sur les points de terminaison Outposts à l'aide des touches AWS Management Console, AWS Command Line Interface (AWS CLI) et. AWS SDK pour Java

Utilisation de la console S3

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts access points (Points d'accès Outposts).
3. Sur la page Outposts access points (Points d'accès des Outposts), sélectionnez l'onglet Outposts endpoints (Points de terminaison des Outposts).
4. Sous Outposts endpoints (Points de terminaison des Outposts), sélectionnez le point de terminaison que vous souhaitez supprimer, puis cliquez sur Delete (Supprimer).

En utilisant le AWS CLI

L' AWS CLI exemple suivant supprime un point de terminaison pour un Outpost. Pour exécuter cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3outposts delete-endpoint --endpoint-id example-endpoint-id --outpost-id op-01ac5d28a6a232904
```

Utilisation du AWS SDK pour Java

L'exemple de kit SDK pour Java suivant illustre la suppression d'un point de terminaison pour un Outpost. Pour utiliser cet exemple, remplacez *user input placeholders* par vos propres informations.

```
import com.amazonaws.arn.Arn;
import com.amazonaws.services.s3outposts.AmazonS3Outposts;
import com.amazonaws.services.s3outposts.AmazonS3OutpostsClientBuilder;
import com.amazonaws.services.s3outposts.model.DeleteEndpointRequest;

public void deleteEndpoint(String endpointArnInput) {
    String outpostId = "op-01ac5d28a6a232904";
    AmazonS3Outposts s3outpostsClient = AmazonS3OutpostsClientBuilder
```

```
        .standard().build();

    Arn endpointArn = Arn.fromString(endpointArnInput);
    String[] resourceParts = endpointArn.getResource().getResource().split("/");
    String endpointId = resourceParts[resourceParts.length - 1];
    DeleteEndpointRequest deleteEndpointRequest = new DeleteEndpointRequest()
        .withEndpointId(endpointId)
        .withOutpostId(outpostId);
    s3OutpostsClient.deleteEndpoint(deleteEndpointRequest);
    System.out.println("Endpoint with id " + endpointId + " is deleted.");
}
```

Utilisation des objets S3 on Outposts

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur APIs les compartiments Outpost que sur les compartiments 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 Command Line Interface (AWS CLI) ou REST. AWS SDKs

Les objets sont les entités fondamentales stockées dans S3 sur Outposts. Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'Amazon Resource Name (ARN) du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN pour les points d'accès S3 sur les Outposts, qui inclut le Région AWS code de la région dans laquelle l'Outpost est hébergé, l'ID, l' Compte AWS ID de l'Outpost et le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur S3 on Outposts ARNs, consultez. [Ressource ARNs pour S3 sur les Outposts](#)

L'objet ARNs utilise le format suivant, qui inclut le lieu Région AWS d'accueil de l'Outpost, son Compte AWS ID, son identifiant, le nom du bucket et la clé de l'objet :

```
arn:aws:s3-outposts:us-west-2:123456789012:outpost/op-01ac5d28a6a232904/bucket/amzn-s3-demo-bucket1/object/myobject
```

Avec Amazon S3 sur Outposts, les données des objets sont toujours stockées sur l'Outpost. Lorsque vous AWS installez un rack Outpost, vos données restent locales dans votre Outpost afin

de répondre aux exigences en matière de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme il AWS Management Console est hébergé dans la région, vous ne pouvez pas utiliser la console pour télécharger ou gérer des objets dans votre Outpost. Cependant, vous pouvez utiliser l'API REST, AWS Command Line Interface (AWS CLI), et AWS SDKs pour télécharger et gérer vos objets via vos points d'accès.

Rubriques

- [Chargement d'un objet dans un compartiment S3 sur Outposts](#)
- [Copier un objet dans un compartiment Amazon S3 on Outposts à l'aide du AWS SDK pour Java](#)
- [Obtenir un objet à partir d'un compartiment Amazon S3 on Outposts](#)
- [Liste des objets dans un compartiment Amazon S3 on Outposts](#)
- [Suppression d'objets dans des compartiments Amazon S3 on Outposts](#)
- [HeadBucket À utiliser pour déterminer si un bucket S3 on Outposts existe et si vous disposez d'autorisations d'accès](#)
- [Réalisation et gestion d'un chargement partitionné avec le kit SDK for Java.](#)
- [Utilisation de Presigned URLs pour S3 sur Outposts](#)
- [Amazon S3 sur Outposts avec Amazon EMR local sur Outposts](#)
- [Mise en cache d'autorisation et d'authentification](#)

Chargement d'un objet dans un compartiment S3 sur Outposts

Les objets sont les entités fondamentales stockées dans S3 sur Outposts. Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'Amazon Resource Name (ARN) du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN pour les points d'accès S3 sur les Outposts, qui inclut le Région AWS code de la région dans laquelle l'Outpost est hébergé, l'ID, l' Compte AWS ID de l'Outpost et le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur S3 on Outposts ARNs, consultez. [Ressource ARNs pour S3 sur les Outposts](#)

Avec Amazon S3 sur Outposts, les données des objets sont toujours stockées sur l'Outpost. Lorsque vous AWS installez un rack Outpost, vos données restent locales dans votre Outpost afin de répondre aux exigences en matière de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme il AWS Management Console est hébergé dans la région, vous ne pouvez pas utiliser la console pour télécharger ou gérer des objets dans votre Outpost. Cependant, vous pouvez utiliser l'API REST, AWS Command Line Interface (AWS CLI), et AWS SDKs pour télécharger et gérer vos objets via vos points d'accès.

Les AWS SDK pour Java exemples suivants AWS CLI vous montrent comment télécharger un objet dans un compartiment S3 on Outposts à l'aide d'un point d'accès.

AWS CLI

Exemple

L'exemple suivant place un objet nommé `sample-object.xml` dans un compartiment S3 sur Outposts (`s3-outposts:PutObject`) à l'aide de l' AWS CLI. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour plus d'informations sur cette commande, consultez [put-object](#) dans la Référence de l'AWS CLI .

```
aws s3api put-object --bucket arn:aws:s3-  
outposts:Region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-  
outposts-access-point --key sample-object.xml --body sample-object.xml
```

SDK for Java

Exemple

Pour des exemples de téléchargement d'un objet dans un bucket S3 Outposts avec le AWS SDK pour Java, consultez [PutObjectOnOutpost.java dans les exemples de code du SDK pour AWS Java 2.x](#).

Copier un objet dans un compartiment Amazon S3 on Outposts à l'aide du AWS SDK pour Java

Les objets sont les entités fondamentales stockées dans S3 on Outposts. Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un

compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'Amazon Resource Name (ARN) du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN pour les points d'accès S3 sur les Outposts, qui inclut le Région AWS code de la région dans laquelle l'Outpost est hébergé, l'ID, l' Compte AWS ID de l'Outpost et le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur S3 on Outposts ARNs, consultez. [Ressource ARNs pour S3 sur les Outposts](#)

Avec Amazon S3 sur Outposts, les données des objets sont toujours stockées sur l'Outpost. Lorsque vous AWS installez un rack Outpost, vos données restent locales dans votre Outpost afin de répondre aux exigences en matière de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme il AWS Management Console est hébergé dans la région, vous ne pouvez pas utiliser la console pour télécharger ou gérer des objets dans votre Outpost. Cependant, vous pouvez utiliser l'API REST, AWS Command Line Interface (AWS CLI), et AWS SDKs pour télécharger et gérer vos objets via vos points d'accès.

L'exemple suivant montre comment copier un objet dans un compartiment S3 on Outposts à l'aide du kit AWS SDK pour Java.

Utilisation du AWS SDK pour Java

L'exemple S3 on Outposts suivant copie un objet dans un nouvel objet situé dans le même compartiment à l'aide du kit 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.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.CopyObjectRequest;

public class CopyObject {
    public static void main(String[] args) {
```

```
String accessPointArn = "*** access point ARN ***";
String sourceKey = "*** Source object key ***";
String destinationKey = "*** Destination object key ***";

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()
        .enableUseArnRegion()
        .build();

    // Copy the object into a new object in the same bucket.
    CopyObjectRequest copyObjectRequest = new CopyObjectRequest(accessPointArn,
sourceKey, accessPointArn, destinationKey);
    s3Client.copyObject(copyObjectRequest);
} 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();
}
}
```

Obtenir un objet à partir d'un compartiment Amazon S3 on Outposts

Les objets sont les entités fondamentales stockées dans S3 sur Outposts. Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'Amazon Resource Name (ARN) du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN pour les points d'accès S3 sur les Outposts, qui inclut le Région AWS code de la région dans laquelle l'Outpost est hébergé, l'ID, l' Compte AWS ID de l'Outpost et le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur S3 on Outposts ARNs, consultez. [Ressource ARNs pour S3 sur les Outposts](#)

Avec Amazon S3 sur Outposts, les données des objets sont toujours stockées sur l'Outpost. Lorsque vous AWS installez un rack Outpost, vos données restent locales dans votre Outpost afin de répondre aux exigences en matière de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme il AWS Management Console est hébergé dans la région, vous ne pouvez pas utiliser la console pour télécharger ou gérer des objets dans votre Outpost. Cependant, vous pouvez utiliser l'API REST, AWS Command Line Interface (AWS CLI), et AWS SDKs pour télécharger et gérer vos objets via vos points d'accès.

Les exemples suivants vous montrent comment télécharger (obtenir) un objet à l'aide de l' AWS Command Line Interface (AWS CLI) et de AWS SDK pour Java.

À l'aide du AWS CLI

L'exemple suivant obtient un objet nommé `sample-object.xml` à partir d'un compartiment S3 on Outposts (`s3-outposts:GetObject`) à l'aide de l' AWS CLI. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour de plus amples informations sur cette commande, veuillez consulter [get-object](#) dans le document AWS CLI Reference.

```
aws s3api get-object --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-access-point --key testkey sample-object.xml
```

Utilisation du AWS SDK pour Java

L'exemple S3 on Outposts suivant obtient un objet à l'aide du kit SDK pour Java. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations. Pour plus d'informations, consultez [GetObject](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.GetObjectRequest;
import com.amazonaws.services.s3.model.ResponseHeaderOverrides;
```

```
import com.amazonaws.services.s3.model.S3Object;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStream;
import java.io.InputStreamReader;

public class GetObject {
    public static void main(String[] args) throws IOException {
        String accessPointArn = "*** access point ARN ***";
        String key = "*** Object key ***";

        S3Object fullObject = null, objectPortion = null, headerOverrideObject = null;
        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()
                .enableUseArnRegion()
                .build();

            // Get an object and print its contents.
            System.out.println("Downloading an object");
            fullObject = s3Client.getObject(new GetObjectRequest(accessPointArn, key));
            System.out.println("Content-Type: " +
fullObject.getObjectMetadata().getContentType());
            System.out.println("Content: ");
            displayTextInputStream(fullObject.getObjectContent());

            // Get a range of bytes from an object and print the bytes.
            GetObjectRequest rangeObjectRequest = new GetObjectRequest(accessPointArn,
key)
                .withRange(0, 9);
            objectPortion = s3Client.getObject(rangeObjectRequest);
            System.out.println("Printing bytes retrieved.");
            displayTextInputStream(objectPortion.getObjectContent());

            // Get an entire object, overriding the specified response headers, and
            print the object's content.
            ResponseHeaderOverrides headerOverrides = new ResponseHeaderOverrides()
                .withCacheControl("No-cache")
                .withContentDisposition("attachment; filename=example.txt");
            GetObjectRequest getObjectRequestHeaderOverride = new
GetObjectRequest(accessPointArn, key)
```

```

        .withResponseHeaders(headerOverrides);
        headerOverrideObject = s3Client.getObject(getObjectRequestHeaderOverride);
        displayTextInputStream(headerOverrideObject.getObjectContent());
    } 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();
    } finally {
        // To ensure that the network connection doesn't remain open, close any
open input streams.
        if (fullObject != null) {
            fullObject.close();
        }
        if (objectPortion != null) {
            objectPortion.close();
        }
        if (headerOverrideObject != null) {
            headerOverrideObject.close();
        }
    }
}

private static void displayTextInputStream(InputStream input) throws IOException {
    // Read the text input stream one line at a time and display each line.
    BufferedReader reader = new BufferedReader(new InputStreamReader(input));
    String line = null;
    while ((line = reader.readLine()) != null) {
        System.out.println(line);
    }
    System.out.println();
}
}

```

Liste des objets dans un compartiment Amazon S3 on Outposts

Les objets sont les entités fondamentales stockées dans S3 on Outposts. Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous

utilisez l'Amazon Resource Name (ARN) du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN pour les points d'accès S3 sur Outposts, qui inclut le code Région AWS pour la région où l'Outpost est hébergé, l'ID Compte AWS, l'ID d'Outpost, le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur les ARN de S3 sur Outposts, consultez [Ressource ARNs pour S3 sur les Outposts](#).

Note

Avec Amazon S3 on Outposts, les données des objets sont toujours stockées sur l'Outpost. Quand AWS installe un rack Outpost, vos données restent locales à votre Outpost pour répondre aux exigences de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme AWS Management Console est hébergé dans la région, vous ne pouvez pas l'utiliser pour charger ou gérer des objets dans votre Outpost. Toutefois, vous pouvez utiliser l'API REST, l'AWS Command Line Interface (AWS CLI) et les kits SDK AWS pour charger et gérer vos objets via vos points d'accès.

Les exemples suivants vous montrent comment répertorier les objets d'un compartiment S3 on Outposts à l'aide de l'AWS CLI et d'AWS SDK pour Java.

Utilisation de l'AWS CLI

L'exemple suivant répertorie les objets dans un compartiment S3 on Outposts (`s3-outposts:ListObjectsV2`) à l'aide de l'AWS CLI. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour de plus amples informations sur cette commande, veuillez consulter [list-objects-v2](#) dans le document AWS CLI Reference.

```
aws s3api list-objects-v2 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-access-point
```

Note

Lorsque vous utilisez cette action avec Amazon S3 sur Outposts via le kit SDK AWS, vous fournissez l'ARN du point d'accès Outposts à la place du nom du compartiment, sous la forme suivante :`arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-Outposts-Access-Point`. Pour plus d'informations sur les ARN de S3 on Outposts, consultez [Ressource ARNs pour S3 sur les Outposts](#).

Utilisation du kit AWS SDK pour Java

L'exemple S3 on Outposts suivant répertorie les objets dans un compartiment à l'aide du kit SDK pour Java. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

Important

Cet exemple utilise [ListObjectsV2](#), qui est la dernière révision de l'opération d'API `ListObjects`. Nous vous recommandons d'utiliser cette opération d'API révisée pour le développement d'applications. Pour des raisons de rétrocompatibilité, Amazon S3 continue de prendre en charge la version précédente de cette opération d'API.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListObjectsV2Request;
import com.amazonaws.services.s3.model.ListObjectsV2Result;
import com.amazonaws.services.s3.model.S3ObjectSummary;

public class ListObjectsV2 {

    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";

        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()
    .enableUseArnRegion()
    .build();

System.out.println("Listing objects");

// maxKeys is set to 2 to demonstrate the use of
// ListObjectsV2Result.getNextContinuationToken()
ListObjectsV2Request req = new
ListObjectsV2Request().withBucketName(accessPointArn).withMaxKeys(2);
ListObjectsV2Result result;

do {
    result = s3Client.listObjectsV2(req);

    for (S3ObjectSummary objectSummary : result.getObjectSummaries()) {
        System.out.printf(" - %s (size: %d)\n", objectSummary.getKey(),
objectSummary.getSize());
    }
    // If there are more than maxKeys keys in the bucket, get a
continuation token
    // and list the next objects.
    String token = result.getNextContinuationToken();
    System.out.println("Next Continuation Token: " + token);
    req.setContinuationToken(token);
} while (result.isTruncated());
} 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();
}
}
```

Suppression d'objets dans des compartiments Amazon S3 on Outposts

Les objets sont les entités fondamentales stockées dans Amazon S3 on Outposts. Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'Amazon Resource Name (ARN) du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN pour les points d'accès S3 sur Outposts, qui inclut le code Région AWS pour la région où l'Outpost est hébergé, l'ID Compte AWS, l'ID d'Outpost, le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur les ARN de S3 sur Outposts, consultez [Ressource ARNs pour S3 sur les Outposts](#).

Avec Amazon S3 on Outposts, les données des objets sont toujours stockées sur l'Outpost. Quand AWS installe un rack Outpost, vos données restent locales à votre Outpost pour répondre aux exigences de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme AWS Management Console est hébergé dans la région, vous ne pouvez pas l'utiliser pour charger ou gérer des objets dans votre Outpost. Toutefois, vous pouvez utiliser l'API REST, AWS Command Line Interface (AWS CLI) et les kits SDK AWS pour charger et gérer vos objets via vos points d'accès.

Les exemples suivants vous montrent comment supprimer un objet unique ou plusieurs objets dans un compartiment S3 on Outposts à l'aide de l'AWS Command Line Interface (AWS CLI) et de AWS SDK pour Java.

Utilisation de l'AWS CLI

Les exemples suivants vous montrent comment supprimer un objet unique ou plusieurs objets d'un compartiment S3 on Outposts.

delete-object

L'exemple suivant supprime un objet nommé `sample-object.xml` d'un compartiment S3 on Outposts (`s3-outposts:DeleteObject`) à l'aide de l'AWS CLI. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour de plus amples informations sur cette commande, veuillez consulter [delete-object](#) dans le document AWS CLI Reference.

```
aws s3api delete-object --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --key sample-object.xml
```

delete-objects

L'exemple suivant supprime deux objets nommés `sample-object.xml` et `test1.txt` d'un compartiment S3 on Outposts (`s3-outposts:DeleteObject`) à l'aide de l'AWS CLI. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour plus d'informations sur cette commande, veuillez consulter [delete-objects](#) dans le document AWS CLI Reference.

```
aws s3api delete-objects --bucket arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point --delete file://delete.json
```

```
delete.json
{
  "Objects": [
    {
      "Key": "test1.txt"
    },
    {
      "Key": "sample-object.xml"
    }
  ],
  "Quiet": false
}
```

Utilisation du kit AWS SDK pour Java

Les exemples suivants vous montrent comment supprimer un objet unique ou plusieurs objets d'un compartiment S3 on Outposts.

DeleteObject

L'exemple S3 on Outposts suivant supprime un objet dans un compartiment à l'aide du kit SDK pour Java. Pour utiliser cet exemple, spécifiez l'ARN du point d'accès pour l'Outpost et le nom de clé de l'objet que vous souhaitez supprimer. Pour plus d'informations, veuillez consulter [DeleteObject](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectRequest;

public class DeleteObject {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String keyName = "*** key name ****";

        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()
                .enableUseArnRegion()
                .build();

            s3Client.deleteObject(new DeleteObjectRequest(accessPointArn, 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();
        }
    }
}
```

```
}
```

DeleteObjects

L'exemple S3 on Outposts suivant télécharge puis supprime des objets dans un compartiment à l'aide du kit SDK pour Java. Pour utiliser cet exemple, spécifiez l'ARN du point d'accès pour l'Outpost. Pour de plus amples informations, veuillez consulter [DeleteObject](#) dans le document Amazon Simple Storage Service API Reference.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.DeleteObjectsRequest;
import com.amazonaws.services.s3.model.DeleteObjectsRequest.KeyVersion;
import com.amazonaws.services.s3.model.DeleteObjectsResult;

import java.util.ArrayList;

public class DeleteObjects {

    public static void main(String[] args) {
        String accessPointArn = "arn:aws:s3-
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-
outposts-access-point";

        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()
                .enableUseArnRegion()
                .build();

            // Upload three sample objects.
            ArrayList<KeyVersion> keys = new ArrayList<KeyVersion>();
            for (int i = 0; i < 3; i++) {
                String keyName = "delete object example " + i;
                s3Client.putObject(accessPointArn, keyName, "Object number " + i + "
to be deleted.");
                keys.add(new KeyVersion(keyName));
            }
        }
    }
}
```

```
        System.out.println(keys.size() + " objects successfully created.");

        // Delete the sample objects.
        DeleteObjectsRequest multiObjectDeleteRequest = new
DeleteObjectsRequest(accessPointArn)
            .withKeys(keys)
            .withQuiet(false);

        // Verify that the objects were deleted successfully.
        DeleteObjectsResult delObjRes =
s3Client.deleteObjects(multiObjectDeleteRequest);
        int successfulDeletes = delObjRes.getDeletedObjects().size();
        System.out.println(successfulDeletes + " objects successfully
deleted.");
    } 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();
    }
}
}
```

HeadBucket À utiliser pour déterminer si un bucket S3 on Outposts existe et si vous disposez d'autorisations d'accès

Les objets sont les entités fondamentales stockées dans Amazon S3 on Outposts. Chaque objet est contenu dans un compartiment. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost. Lorsque vous spécifiez le compartiment pour les opérations d'objet, vous utilisez l'Amazon Resource Name (ARN) du point d'accès ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

L'exemple suivant montre le format ARN pour les points d'accès S3 sur les Outposts, qui inclut le Région AWS code de la région dans laquelle l'Outpost est hébergé, l'ID, l' Compte AWS ID de l'Outpost et le nom du point d'accès :

```
arn:aws:s3-outposts:region:account-id:outpost/outpost-id/accesspoint/accesspoint-name
```

Pour plus d'informations sur S3 on Outposts ARNs, consultez. [Ressource ARNs pour S3 sur les Outposts](#)

Note

Avec Amazon S3 sur Outposts, les données des objets sont toujours stockées sur l'Outpost. Lorsque vous AWS installez un rack Outpost, vos données restent locales dans votre Outpost afin de répondre aux exigences de résidence des données. Vos objets ne quittent jamais votre Outpost et ne se trouvent pas dans un Région AWS. Comme il AWS Management Console est hébergé dans la région, vous ne pouvez pas utiliser la console pour télécharger ou gérer des objets dans votre Outpost. Cependant, vous pouvez utiliser l'API REST, AWS Command Line Interface (AWS CLI), et AWS SDKs pour télécharger et gérer vos objets via vos points d'accès.

Les AWS SDK pour Java exemples suivants AWS Command Line Interface (AWS CLI) vous montrent comment utiliser l'opération d' HeadBucketAPI pour déterminer si un bucket Amazon S3 on Outposts existe et si vous êtes autorisé à y accéder. Pour plus d'informations, consultez [HeadBucket](#) dans la Référence d'API Amazon Simple Storage Service.

En utilisant le AWS CLI

L' AWS CLI exemple suivant de S3 on Outposts utilise la head-bucket commande pour déterminer si un bucket existe et si vous êtes autorisé à y accéder. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour de plus amples informations sur cette commande, veuillez consulter [head-bucket](#) dans le document AWS CLI Reference.

```
aws s3api head-bucket --bucket arn:aws:s3-  
outposts:region:123456789012:outpost/op-01ac5d28a6a232904/accesspoint/example-outposts-  
access-point
```

Utilisation du AWS SDK pour Java

L'exemple suivant de S3 on Outposts montre comment déterminer si un compartiment existe et si vous avez l'autorisation d'y accéder. Pour utiliser cet exemple, spécifiez l'ARN du point d'accès pour

l'Outpost. Pour plus d'informations, consultez [HeadBucket](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.HeadBucketRequest;

public class HeadBucket {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";

        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()
                .enableUseArnRegion()
                .build();

            s3Client.headBucket(new HeadBucketRequest(accessPointArn));
        } 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();
        }
    }
}
```

Réalisation et gestion d'un chargement partitionné avec le kit SDK for Java.

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 S3 sur Outposts via l'API AWS Management Console, AWS Command Line Interface (AWS

CLI) ou REST. AWS SDKs Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Les exemples suivants montrent comment vous pouvez utiliser S3 sur Outposts AWS SDK pour Java pour effectuer et gérer un téléchargement partitionné.

Rubriques

- [Effectuer le chargement partitionné d'un objet dans un compartiment S3 sur Outposts](#)
- [Copie d'un objet de grande taille dans un compartiment S3 sur Outposts à l'aide du chargement partitionné](#)
- [Générer une liste des parties d'un objet dans un compartiment S3 sur Outposts](#)
- [Récupérer une liste de chargements partitionnés en cours dans un compartiment S3 sur Outposts](#)

Effectuer le chargement partitionné d'un objet dans un compartiment S3 sur Outposts

L'exemple S3 sur Outposts suivant lance, télécharge et achève le chargement partitionné d'un objet dans un compartiment à l'aide du kit SDK pour Java. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations. Pour plus d'informations, consultez [Chargement d'un objet à l'aide du chargement partitionné](#) dans le Guide de l'utilisateur Amazon Simple Storage Service.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.ArrayList;
import java.util.List;

public class MultipartUploadCopy {
    public static void main(String[] args) {
        String accessPointArn = "*** Source access point ARN ***";
        String sourceObjectKey = "*** Source object key ***";
        String destObjectKey = "*** Target object key ***";

        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()
    .enableUseArnRegion()
    .build();

// Initiate the multipart upload.
InitiateMultipartUploadRequest initRequest = new
InitiateMultipartUploadRequest(accessPointArn, destObjectKey);
InitiateMultipartUploadResult initResult =
s3Client.initiateMultipartUpload(initRequest);

// Get the object size to track the end of the copy operation.
GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest(accessPointArn, 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(accessPointArn)
        .withSourceKey(sourceObjectKey)
        .withDestinationBucketName(accessPointArn)
        .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(
            accessPointArn,
            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;
}
```

Copie d'un objet de grande taille dans un compartiment S3 sur Outposts à l'aide du chargement partitionné

L'exemple S3 sur Outposts suivant copie un objet dans un compartiment à l'aide du kit SDK pour Java. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;
```

```
import java.util.ArrayList;
import java.util.List;

public class MultipartUploadCopy {
    public static void main(String[] args) {
        String accessPointArn = "*** Source access point ARN ***";
        String sourceObjectKey = "*** Source object key ***";
        String destObjectKey = "*** Target object key ***";

        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()
                .enableUseArnRegion()
                .build();

            // Initiate the multipart upload.
            InitiateMultipartUploadRequest initRequest = new
InitiateMultipartUploadRequest(accessPointArn, destObjectKey);
            InitiateMultipartUploadResult initResult =
s3Client.initiateMultipartUpload(initRequest);

            // Get the object size to track the end of the copy operation.
            GetObjectMetadataRequest metadataRequest = new
GetObjectMetadataRequest(accessPointArn, 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(accessPointArn)
```

```
        .withSourceKey(sourceObjectKey)
        .withDestinationBucketName(accessPointArn)
        .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(
    accessPointArn,
    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;
}
}
```

Générer une liste des parties d'un objet dans un compartiment S3 sur Outposts

L'exemple S3 sur Outposts suivant répertorie les parties d'un objet dans un compartiment à l'aide du kit SDK pour Java. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.*;

import java.util.List;

public class ListParts {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";
        String keyName = "*** Key name ***";
        String uploadId = "*** Upload ID ***";

        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()
                .enableUseArnRegion()
                .build();

            ListPartsRequest listPartsRequest = new ListPartsRequest(accessPointArn,
keyName, uploadId);
            PartListing partListing = s3Client.listParts(listPartsRequest);
            List<PartSummary> partSummaries = partListing.getParts();

            System.out.println(partSummaries.size() + " multipart upload parts");
            for (PartSummary p : partSummaries) {
                System.out.println("Upload part: Part number = \"" + p.getPartNumber()
+ "\", ETag = " + p.getETag());
            }

        } 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();
    }
}
}
```

Récupérer une liste de chargements partitionnés en cours dans un compartiment S3 sur Outposts

L'exemple S3 sur Outposts suivant montre comment récupérer une liste de chargements partitionnés en cours à partir d'un compartiment Outposts à l'aide du kit SDK pour Java. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import com.amazonaws.services.s3.AmazonS3;
import com.amazonaws.services.s3.AmazonS3ClientBuilder;
import com.amazonaws.services.s3.model.ListMultipartUploadsRequest;
import com.amazonaws.services.s3.model.MultipartUpload;
import com.amazonaws.services.s3.model.MultipartUploadListing;

import java.util.List;

public class ListMultipartUploads {
    public static void main(String[] args) {
        String accessPointArn = "*** access point ARN ***";

        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()
                .enableUseArnRegion()
                .build();

            // Retrieve a list of all in-progress multipart uploads.
            ListMultipartUploadsRequest allMultipartUploadsRequest = new
            ListMultipartUploadsRequest(accessPointArn);
```

```
        MultipartUploadListing multipartUploadListing =
s3Client.listMultipartUploads(allMultipartUploadsRequest);
        List<MultipartUpload> uploads =
multipartUploadListing.getMultipartUploads();

        // Display information about all in-progress multipart uploads.
        System.out.println(uploads.size() + " multipart upload(s) in progress.");
        for (MultipartUpload u : uploads) {
            System.out.println("Upload in progress: Key = \"\" + u.getKey() + "\",
id = \"\" + u.getUploadId());
        }
    } 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();
    }
}
}
```

Utilisation de Presigned URLs pour S3 sur Outposts

Pour accorder un accès limité dans le temps aux objets stockés localement dans un Outpost sans mettre à jour votre stratégie de compartiment, vous pouvez utiliser une URL présignée. Avec Presigned URLs, en tant que propriétaire du bucket, vous pouvez partager des objets avec des personnes dans votre cloud privé virtuel (VPC) ou leur donner la possibilité de télécharger ou de supprimer des objets.

Lorsque vous créez une URL présignée à l'aide du AWS SDKs ou du AWS Command Line Interface (AWS CLI), vous associez l'URL à une action spécifique. Vous accordez également un accès limité dans le temps à l'URL présignée en choisissant un délai d'expiration personnalisé qui peut aller de 1 seconde à 7 jours. Lorsque vous partagez l'URL présignée, la personne dans le VPC peut effectuer l'action intégrée dans l'URL comme s'il s'agissait de l'utilisateur connecté d'origine. Lorsque l'URL atteint son délai d'expiration, elle expire et ne fonctionne plus.

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.

AWS Version 4 de la signature (SigV4)

Pour appliquer un comportement spécifique lorsque les demandes d'URL présignées sont authentifiées à l'aide de AWS Signature Version 4 (SigV4), vous pouvez utiliser des clés de condition dans les politiques de compartiment et les politiques de point d'accès. Par exemple, vous pouvez créer une stratégie de compartiment qui utilise la condition `s3-outposts:signatureAge` pour refuser toute demande d'URL présignée Amazon S3 on Outposts sur les objets du compartiment `example-outpost-bucket` si la signature date de plus de 10 minutes. Pour utiliser cet exemple, remplacez les *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
minutes old",
      "Effect": "Deny",
      "Principal": {"AWS": "444455556666"},
      "Action": "s3-outposts:*",
      "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
      "Condition": {
        "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
        "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
      }
    }
  ]
}
```

Pour obtenir la liste des clés de condition et des exemples de stratégies supplémentaires que vous pouvez utiliser pour imposer un comportement spécifique lorsque des requêtes d'URL présignées

sont authentifiées à l'aide de Signature Version 4, consultez [AWS Clés de politique spécifiques à l'authentification Signature Version 4 \(SigV4\)](#).

Restriction de chemin réseau

Si vous souhaitez restreindre l'utilisation de l'accès présigné URLs et de tous les accès S3 on Outposts à des chemins réseau particuliers, vous pouvez écrire des politiques qui nécessitent un chemin réseau particulier. Pour définir la restriction sur le principal IAM qui effectue l'appel, vous pouvez utiliser des politiques basées sur l'identité Gestion des identités et des accès AWS (IAM) (par exemple, des politiques d'utilisateur, de groupe ou de rôle). Pour définir la restriction de la ressource S3 on Outposts, vous pouvez utiliser des stratégies basées sur les ressources (par exemple, des stratégies de compartiment et de point d'accès).

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 condition globale IAM que vous utilisez dépend du type de point de terminaison. Si vous utilisez le point de terminaison public pour S3 on Outposts, utilisez `aws:SourceIp`. Si vous utilisez le point de terminaison d'un VPC pour S3 sur Outposts, 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, même lorsqu'une personne utilise une URL présignée pour S3 on Outposts. Pour utiliser cet exemple, remplacez les *user input placeholders* par vos propres informations.

```
{
  "Sid": "NetworkRestrictionForIAMPrincipal",
  "Effect": "Deny",
  "Action": "*",
  "Resource": "*",
  "Condition": {
    "NotIpAddressIfExists": {"aws:SourceIp": "IP-address-range"},
    "BoolIfExists": {"aws:ViaAWSService": "false"}
  }
}
```

Pour un exemple de politique de compartiment qui utilise la clé de condition `aws:SourceIP` AWS globale pour restreindre l'accès à un compartiment S3 on Outposts à une plage réseau spécifique, consultez [Configuration d'IAM avec S3 sur Outposts](#)

Utilisateurs habilités à créer une URL présignée

Toute personne qui possède des autorisations de sécurité valides peut créer une URL présignée. Mais pour qu'un utilisateur dans le VPC 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.

Vous pouvez utiliser les informations d'identification suivantes pour créer une URL présignée :

- Profil d'instance IAM : valide pendant 6 heures.
- AWS Security Token Service : valide pendant 36 heures lorsque signé avec des autorisations permanentes, telles que les autorisations de l'utilisateur root du Compte AWS ou d'un utilisateur IAM.
- Utilisateur IAM — Valable jusqu'à 7 jours lorsque vous utilisez AWS Signature version 4.

Afin de créer une URL présignée valide pendant 7 jours, commencez par déléguer des autorisations d'utilisateur IAM (clé d'accès et clé secrète) pour le kit SDK que vous utilisez. Générez ensuite une URL présignée à l'aide de la version 4 de la AWS signature.

Note

- Si vous avez créé une URL présignée à l'aide d'un jeton temporaire, l'URL expire lorsque le jeton expire, même si vous avez créé l'URL avec une heure d'expiration postérieure.
- Dans la mesure où URLs les buckets S3 on Outposts sont autorisés à accéder à ceux qui possèdent l'URL, nous vous recommandons de les protéger de manière appropriée. Pour plus d'informations sur la protection des documents présignés URLs, consultez [Limitation des capacités des URL présignées](#).

Quand S3 on Outposts vérifie-t-il la date et l'heure d'expiration dans une URL présignée ?

S3 on Outposts 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.

Pour plus d'informations sur l'utilisation d'une URL présignée pour partager ou charger des objets, consultez les rubriques suivantes.

Rubriques

- [Partage d'objets à l'aide d'une signature préalable URLs](#)
- [Génération d'une URL présignée pour charger un objet sur un compartiment S3 on Outposts](#)

Partage d'objets à l'aide d'une signature préalable URLs

Pour accorder un accès limité dans le temps aux objets stockés localement dans un Outpost sans mettre à jour votre stratégie de compartiment, vous pouvez utiliser une URL présignée. Avec Presigned URLs, en tant que propriétaire du bucket, vous pouvez partager des objets avec des personnes dans votre cloud privé virtuel (VPC) ou leur donner la possibilité de télécharger ou de supprimer des objets.

Lorsque vous créez une URL présignée à l'aide du AWS SDKs ou du AWS Command Line Interface (AWS CLI), vous associez l'URL à une action spécifique. Vous accordez également un accès limité dans le temps à l'URL présignée en choisissant un délai d'expiration personnalisé qui peut aller de 1 seconde à 7 jours. Lorsque vous partagez l'URL présignée, la personne dans le VPC peut effectuer l'action intégrée dans l'URL comme s'il s'agissait de l'utilisateur connecté d'origine. Lorsque l'URL atteint son délai d'expiration, elle expire et ne fonctionne plus.

Lorsque vous créez une URL présignée, vous devez fournir vos informations d'identification de sécurité, puis spécifier les éléments suivants :

- Un point d'accès pour Amazon Resource Name (ARN) du compartiment S3 on Outposts
- Une clé d'objet
- Une méthode HTTP (GET pour télécharger des objets)
- Une date et une heure d'expiration

Une URL présignée est uniquement valide pendant la durée spécifiée. Autrement dit, vous devez commencer l'action autorisée par l'URL avant la date et l'heure d'expiration. Vous pouvez utiliser une URL présignée plusieurs fois, jusqu'à la date et l'heure d'expiration. Si vous avez créé une URL

présignée à l'aide d'un jeton temporaire, alors l'URL expire lorsque le jeton expire, même si vous avez créé l'URL avec une heure d'expiration postérieure.

Les utilisateurs du cloud privé virtuel (VPC) qui ont accès à l'URL présignée peuvent accéder à l'objet. Par exemple, si votre compartiment contient une vidéo et que ce compartiment et l'objet sont confidentiels, vous pouvez partager la vidéo avec d'autres en générant une URL présignée. Dans la mesure où URLs les buckets S3 on Outposts sont autorisés à accéder à ceux qui possèdent l'URL, nous vous recommandons de les protéger de manière appropriée. URLs Pour plus de détails sur la protection des documents présignés URLs, consultez [Limitation des capacités des URL présignées](#).

Toute personne qui possède des autorisations de sécurité valides peut créer une URL présignée. Cependant, l'URL présignée doit être créée par une personne disposant des autorisations nécessaires pour effectuer l'opération sur laquelle l'URL présignée est basée. Pour de plus amples informations, veuillez consulter [Utilisateurs habilités à créer une URL présignée](#).

Vous pouvez générer une URL présignée pour partager un objet dans un compartiment S3 on Outposts en utilisant AWS SDKs le et le. AWS CLI Pour plus d'informations, consultez les exemples suivants.

En utilisant le AWS SDKs

Vous pouvez utiliser le AWS SDKs pour générer une URL présignée que vous pouvez communiquer à d'autres personnes afin qu'elles puissent récupérer un objet.

Note

Lorsque vous utilisez le AWS SDKs pour générer une URL présignée, le délai d'expiration maximal d'une URL présignée est de 7 jours à compter de sa création.

Java

Exemple

L'exemple suivant génère une URL présignée que vous pouvez communiquer à d'autres afin qu'ils puissent récupérer un objet depuis un compartiment S3 sur Outposts. Pour de plus amples informations, veuillez consulter [Utilisation de Presigned URLs pour S3 sur Outposts](#). Pour utiliser cet exemple, remplacez les *user input placeholders* par vos propres informations.

```
import com.amazonaws.AmazonServiceException;  
import com.amazonaws.HttpMethod;
```

```
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.GeneratePresignedUrlRequest;

import java.io.IOException;
import java.net.URL;
import java.time.Instant;

public class GeneratePresignedURL {

    public static void main(String[] args) throws IOException {
        Regions clientRegion = Regions.DEFAULT_REGION;
        String accessPointArn = "*** access point ARN ***";
        String objectKey = "*** object key ***";

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

            // Set the presigned URL to expire after one hour.
            java.util.Date expiration = new java.util.Date();
            long expTimeMillis = Instant.now().toEpochMilli();
            expTimeMillis += 1000 * 60 * 60;
            expiration.setTime(expTimeMillis);

            // Generate the presigned URL.
            System.out.println("Generating pre-signed URL.");
            GeneratePresignedUrlRequest generatePresignedUrlRequest =
                new GeneratePresignedUrlRequest(accessPointArn, objectKey)
                    .withMethod(HttpMethod.GET)
                    .withExpiration(expiration);
            URL url = s3Client.generatePresignedUrl(generatePresignedUrlRequest);

            System.out.println("Pre-Signed URL: " + url.toString());
        } 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

L'exemple suivant génère une URL présignée que vous pouvez communiquer à d'autres afin qu'ils puissent récupérer un objet depuis un compartiment S3 sur Outposts. Pour de plus amples informations, veuillez consulter [Utilisation de Presigned URLs pour S3 sur Outposts](#). Pour utiliser cet exemple, remplacez les *user input placeholders* par vos propres informations.

```
using Amazon;  
using Amazon.S3;  
using Amazon.S3.Model;  
using System;  
  
namespace Amazon.DocSamples.S3  
{  
    class GenPresignedURLTest  
    {  
        private const string accessPointArn = "*** access point ARN ***";  
        private const string objectKey = "*** object key ***";  
        // Specify how long the presigned URL lasts, in hours.  
        private const double timeoutDuration = 12;  
        // 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);  
            string urlString = GeneratePreSignedURL(timeoutDuration);  
        }  
        static string GeneratePreSignedURL(double duration)  
        {
```

```
        string urlString = "";
        try
        {
            GetPreSignedUrlRequest request1 = new GetPreSignedUrlRequest
            {
                BucketName = accessPointArn,
                Key = objectKey,
                Expires = DateTime.UtcNow.AddHours(duration)
            };
            urlString = s3Client.GetPreSignedURL(request1);
        }
        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);
        }
        return urlString;
    }
}
```

Python

L'exemple suivant génère une URL présignée pour partager un objet à l'aide du SDK pour Python (Boto3). Par exemple, utilisez un client Boto3 et la fonction `generate_presigned_url` pour générer une URL présignée qui vous permet d'accéder à un objet GET.

```
import boto3
url = boto3.client('s3').generate_presigned_url(
    ClientMethod='get_object',
    Params={'Bucket': 'ACCESS_POINT_ARN', 'Key': 'OBJECT_KEY'},
    ExpiresIn=3600)
```

Pour plus d'informations sur l'utilisation du kit SDK pour Python (Boto3) pour générer une URL présignée, consultez la section [Python](#) dans la Référence d'API AWS SDK pour Python (Boto) .

En utilisant le AWS CLI

L'exemple de AWS CLI commande suivant génère une URL présignée pour un compartiment S3 on Outposts. Pour utiliser cet exemple, remplacez les *user input placeholders* par vos propres informations.

Note

Lorsque vous utilisez le AWS CLI pour générer une URL présignée, le délai d'expiration maximal d'une URL présignée est de 7 jours à compter de sa création.

```
aws s3 presign s3://arn:aws:s3-outposts:us-east-1:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/example-outpost-access-point/mydoc.txt --expires-in 604800
```

Pour de plus amples informations, veuillez consulter [presign](#) (présigner) dans la Référence des commandes AWS CLI .

Génération d'une URL présignée pour charger un objet sur un compartiment S3 on Outposts

Pour accorder un accès limité dans le temps aux objets stockés localement dans un Outpost sans mettre à jour votre stratégie de compartiment, vous pouvez utiliser une URL présignée. Avec Presigned URLs, en tant que propriétaire du bucket, vous pouvez partager des objets avec des personnes dans votre cloud privé virtuel (VPC) ou leur donner la possibilité de télécharger ou de supprimer des objets.

Lorsque vous créez une URL présignée à l'aide du AWS SDKs ou du AWS Command Line Interface (AWS CLI), vous associez l'URL à une action spécifique. Vous accordez également un accès limité dans le temps à l'URL présignée en choisissant un délai d'expiration personnalisé qui peut aller de 1 seconde à 7 jours. Lorsque vous partagez l'URL présignée, la personne dans le VPC peut effectuer l'action intégrée dans l'URL comme s'il s'agissait de l'utilisateur connecté d'origine. Lorsque l'URL atteint son délai d'expiration, elle expire et ne fonctionne plus.

Lorsque vous créez une URL présignée, vous devez fournir vos informations d'identification de sécurité, puis spécifier les éléments suivants :

- Un point d'accès pour Amazon Resource Name (ARN) du compartiment S3 on Outposts

- Une clé d'objet
- Une méthode HTTP (PUT pour le chargement d'objets)
- Une date et une heure d'expiration

Une URL présignée est uniquement valide pendant la durée spécifiée. Autrement dit, vous devez commencer l'action autorisée par l'URL avant la date et l'heure d'expiration. Vous pouvez utiliser une URL présignée plusieurs fois, jusqu'à la date et l'heure d'expiration. Si vous avez créé une URL présignée à l'aide d'un jeton temporaire, alors l'URL expire lorsque le jeton expire, même si vous avez créé l'URL avec une heure d'expiration postérieure.

Si l'action autorisée par l'URL présignée est composée de plusieurs étapes, comme un chargement partitionné, vous devez démarrer l'ensemble des étapes avant l'expiration. Si S3 on Outposts tente de démarrer une étape avec une URL expirée, vous recevrez une erreur.

Les utilisateurs du cloud privé virtuel (VPC) qui ont accès à l'URL présignée peuvent charger des objets. Par exemple, un utilisateur du VPC qui a accès à l'URL présignée peut charger un objet dans votre compartiment. Étant donné que la version présignée URLs accorde l'accès à votre bucket S3 on Outposts à tout utilisateur du VPC ayant accès à l'URL présignée, nous vous recommandons de protéger ces URL de manière appropriée. Pour plus de détails sur la protection des documents présignés URLs, consultez [Limitation des capacités des URL présignées](#).

Toute personne qui possède des autorisations de sécurité valides peut créer une URL présignée. Cependant, l'URL présignée doit être créée par une personne disposant des autorisations nécessaires pour effectuer l'opération sur laquelle l'URL présignée est basée. Pour de plus amples informations, veuillez consulter [Utilisateurs habilités à créer une URL présignée](#).

Utilisation du AWS SDKs pour générer une URL présignée pour une opération d'objet S3 on Outposts

Java

SDK pour Java 2.x

Cet exemple montre comment générer une URL présignée que vous pouvez utiliser pour charger un objet dans un compartiment S3 on Outposts pour une durée limitée. Pour de plus amples informations, veuillez consulter [Utilisation de Presigned URLs pour S3 sur Outposts](#).

```
public static void signBucket(S3Presigner presigner, String
outpostAccessPointArn, String keyName) {
```

```
try {
    PutObjectRequest objectRequest = PutObjectRequest.builder()
        .bucket(accessPointArn)
        .key(keyName)
        .contentType("text/plain")
        .build();

    PutObjectPresignRequest presignRequest =
PutObjectPresignRequest.builder()
        .signatureDuration(Duration.ofMinutes(10))
        .putObjectRequest(objectRequest)
        .build();

    PresignedPutObjectRequest presignedRequest =
presigner.presignPutObject(presignRequest);

    String myURL = presignedRequest.url().toString();
    System.out.println("Presigned URL to upload a file to: " +myURL);
    System.out.println("Which HTTP method must be used when uploading a
file: " +
        presignedRequest.httpRequest().method());

    // Upload content to the S3 on Outposts bucket by using this URL.
    URL url = presignedRequest.url();

    // Create the connection and use it to upload the new object by using
the presigned URL.
    HttpURLConnection connection = (HttpURLConnection)
url.openConnection();
    connection.setDoOutput(true);
    connection.setRequestProperty("Content-Type", "text/plain");
    connection.setRequestMethod("PUT");
    OutputStreamWriter out = new
OutputStreamWriter(connection.getOutputStream());
    out.write("This text was uploaded as an object by using a presigned
URL.");
    out.close();

    connection.getResponseCode();
    System.out.println("HTTP response code is " +
connection.getResponseCode());
}
```

```
    } catch (S3Exception e) {
        e.printStackTrace();
    } catch (IOException e) {
        e.printStackTrace();
    }
}
```

Python

Kit SDK for Python (Boto3)

Cet exemple montre comment générer une URL présignée qui peut exécuter une action S3 on Outposts pour une durée limitée. Pour de plus amples informations, veuillez consulter [Utilisation de Presigned URLs pour S3 sur Outposts](#). Pour effectuer une requête avec l'URL, utilisez le package Requests.

```
import argparse
import logging
import boto3
from botocore.exceptions import ClientError
import requests

logger = logging.getLogger(__name__)

def generate_presigned_url(s3_client, client_method, method_parameters,
    expires_in):
    """
    Generate a presigned S3 on Outposts 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 that 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
```

```
    )
    logger.info("Got presigned URL: %s", url)
except ClientError:
    logger.exception(
        "Couldn't get a presigned URL for client method '%s'.",
client_method)
    raise
return url

def usage_demo():
    logging.basicConfig(level=logging.INFO, format='%(levelname)s: %(message)s')

    print('-'*88)
    print("Welcome to the Amazon S3 on Outposts presigned URL demo.")
    print('-'*88)

    parser = argparse.ArgumentParser()
    parser.add_argument('accessPointArn', help="The name of the S3 on Outposts
access point ARN.")
    parser.add_argument(
        'key', help="For a GET operation, the key of the object in S3 on
Outposts. For a "
            "PUT operation, the name of a file to upload.")
    parser.add_argument(
        'action', choices=('get', 'put'), help="The action to perform.")
    args = parser.parse_args()

    s3_client = boto3.client('s3')
    client_action = 'get_object' if args.action == 'get' else 'put_object'
    url = generate_presigned_url(
        s3_client, client_action, {'Bucket': args.accessPointArn, 'Key':
args.key}, 1000)

    print("Using the Requests package to send a request to the URL.")
    response = None
    if args.action == 'get':
        response = requests.get(url)
    elif args.action == 'put':
        print("Putting data to the URL.")
        try:
            with open(args.key, 'r') as object_file:
                object_text = object_file.read()
            response = requests.put(url, data=object_text)
```

```
except FileNotFoundError:
    print(f"Couldn't find {args.key}. For a PUT operation, the key must
be the "
        f"name of a file that exists on your computer.")

if response is not None:
    print("Got response:")
    print(f"Status: {response.status_code}")
    print(response.text)

print('-'*88)

if __name__ == '__main__':
    usage_demo()
```

Amazon S3 sur Outposts avec Amazon EMR local sur Outposts

Amazon EMR est une plate-forme de cluster gérée qui simplifie l'exécution de structures de mégadonnées, telles que le traitement Apache Hadoop et Apache Spark AWS 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'analytique et pour des charges de travail d'informatique décisionnelle. Amazon EMR vous aide également à transformer et à déplacer de grandes quantités de données vers et depuis d'autres banques de données et bases de AWS données, et prend en charge Amazon S3 on Outposts. Pour plus d'informations sur Amazon EMR, consultez [Amazon EMR sur Outposts](#) dans le Guide de gestion Amazon EMR.

Pour Amazon S3 sur Outposts, Amazon EMR a commencé à prendre en charge le connecteur Apache Hadoop S3A dans sa version 7.0.0. Les versions antérieures d'Amazon EMR ne prennent pas en charge le service S3 local sur Outposts, et le système de fichiers EMR (EMRFS) n'est pas pris en charge.

Applications prises en charge

Amazon EMR avec Amazon S3 sur Outposts prend en charge les applications suivantes :

- Hadoop
- Spark
- Hue

- Hive
- Sqoop
- Pig
- Hudi
- Flink

Pour plus d'informations, consultez le [Guide de version Amazon EMR](#).

Création et configuration d'un compartiment Amazon S3 sur Outposts

Amazon EMR utilise Amazon S3 on Outposts pour stocker les données d'entrée et de sortie. AWS SDK pour Java Vos fichiers journaux Amazon EMR sont stockés dans un emplacement Amazon S3 régional que vous sélectionnez et ne sont pas stockés localement sur l'Outpost. Pour plus d'informations, consultez [Journaux Amazon EMR](#) dans le Guide de gestion Amazon EMR.

Pour se conformer aux exigences Amazon S3 et DNS, les compartiments S3 sur Outposts sont soumis à des restrictions et des limitations. Pour de plus amples informations, veuillez consulter [Création d'un compartiment S3 sur Outposts](#).

À partir d'Amazon EMR version 7.0.0, vous pouvez utiliser Amazon EMR avec S3 sur Outposts et le système de fichiers S3A.

Prérequis

Autorisations S3 on Outposts — Lorsque vous créez votre profil d'instance Amazon EMR, votre rôle doit contenir l'espace de noms Gestion des identités et des accès AWS (IAM) de S3 on Outposts. S3 sur Outposts possède son propre espace de noms, `s3-outposts*`. Pour obtenir un exemple de politique utilisant cet espace de noms, consultez [Configuration d'IAM avec S3 sur Outposts](#).

Connecteur S3A : pour configurer votre cluster EMR pour accéder aux données d'un compartiment Amazon S3 sur Outposts, vous devez utiliser le connecteur Apache Hadoop S3A. Pour utiliser le connecteur, assurez-vous que tous vos S3 URIs utilisent le `s3a` schéma. Si ce n'est pas le cas, vous pouvez configurer l'implémentation du système de fichiers que vous utilisez pour votre cluster EMR afin que votre S3 URIs fonctionne avec le connecteur S3A.

Pour configurer l'implémentation du système de fichiers afin qu'elle fonctionne avec le connecteur S3A, vous utilisez les propriétés de `fs.AbstractFileSystem.file_scheme.impl` configuration `fs.file_scheme.impl` et de votre cluster EMR, `file_scheme` qui correspondent au type de URIs

S3 dont vous disposez. Pour utiliser l'exemple suivant, remplacez les *user input placeholders* par vos propres informations. Par exemple, pour modifier l'implémentation du système de fichiers pour S3 URIs qui utilise le s3 schéma, spécifiez les propriétés de configuration de cluster suivantes :

```
[
  {
    "Classification": "core-site",
    "Properties": {
      "fs.s3.impl": "org.apache.hadoop.fs.s3a.S3AFileSystem",
      "fs.AbstractFileSystem.s3.impl": "org.apache.hadoop.fs.s3a.S3A"
    }
  }
]
```

Pour utiliser S3A, définissez la propriété de configuration `fs.file_scheme.impl` sur `org.apache.hadoop.fs.s3a.S3AFileSystem` et définissez la propriété `fs.AbstractFileSystem.file_scheme.impl` sur `org.apache.hadoop.fs.s3a.S3A`.

Par exemple, si vous accédez au chemin `s3a://bucket/...`, définissez la propriété `fs.s3a.impl` sur `org.apache.hadoop.fs.s3a.S3AFileSystem` et définissez la propriété `fs.AbstractFileSystem.s3a.impl` sur `org.apache.hadoop.fs.s3a.S3A`.

Premiers pas avec Amazon EMR et Amazon S3 sur Outposts

Les rubriques suivantes expliquent comment commencer à utiliser Amazon EMR avec Amazon S3 sur Outposts.

Rubriques

- [Création d'une stratégie d'autorisations](#)
- [Création et configuration de votre cluster](#)
- [Présentation des configurations](#)
- [Considérations](#)

Création d'une stratégie d'autorisations

Avant de créer un cluster EMR utilisant Amazon S3 sur Outposts, vous devez créer une politique IAM à attacher au profil d'instance Amazon EC2 pour le cluster. Cette politique doit disposer

d'autorisations pour accéder à l'Amazon Resource Name (ARN) du point d'accès S3 sur Outposts. Pour plus d'informations sur la création de politiques IAM pour S3 sur Outposts, consultez [Configuration d'IAM avec S3 sur Outposts](#).

L'exemple de politique suivant montre comment accorder les autorisations requises. Après avoir créé la politique, associez-la au rôle de profil d'instance que vous utilisez pour créer votre cluster EMR, comme décrit dans la section [the section called "Création et configuration de votre cluster"](#). Pour utiliser cet exemple, remplacez les *user input placeholders* par vos propres informations.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Resource": "arn:aws:s3-outposts:us-
west-2:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name",
      "Action": [
        "s3-outposts:*"
      ]
    }
  ]
}
```

Création et configuration de votre cluster

Pour créer un cluster qui exécute Spark avec S3 sur Outposts, procédez comme suit dans la console.

Pour créer un cluster qui exécute Spark avec S3 sur Outposts

1. Ouvrez la console Amazon EMR à l'adresse <https://console.aws.amazon.com/elasticmapreduce/>.
2. Dans le volet de navigation de gauche, choisissez Clusters.
3. Choisissez Créer un cluster.
4. Pour Version Amazon EMR, choisissez emr-7.0.0 ou une version ultérieure.
5. Pour Offre d'applications, choisissez Spark interactive. Sélectionnez ensuite les autres applications prises en charge que vous souhaitez inclure dans votre cluster.
6. Pour activer Amazon S3 sur Outposts, entrez vos paramètres de configuration.

Exemples de paramètres de configuration

Pour utiliser les exemples de paramètres de configuration suivants, remplacez les *user input placeholders* par vos propres informations.

```
[
  {
    "Classification": "core-site",
    "Properties": {
      "fs.s3a.bucket.DOC-EXAMPLE-BUCKET.accesspoint.arn": "arn:aws:s3-outposts:us-
west-2:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/access-point-name"
      "fs.s3a.committer.name": "magic",
      "fs.s3a.select.enabled": "false"
    }
  },
  {
    "Classification": "hadoop-env",
    "Configurations": [
      {
        "Classification": "export",
        "Properties": {
          "JAVA_HOME": "/usr/lib/jvm/java-11-amazon-corretto.x86_64"
        }
      }
    ],
    "Properties": {}
  },
  {
    "Classification": "spark-env",
    "Configurations": [
      {
        "Classification": "export",
        "Properties": {
          "JAVA_HOME": "/usr/lib/jvm/java-11-amazon-corretto.x86_64"
        }
      }
    ],
    "Properties": {}
  },
  {
    "Classification": "spark-defaults",
    "Properties": {
      "spark.executorEnv.JAVA_HOME": "/usr/lib/jvm/java-11-amazon-
corretto.x86_64",
```

```

        "spark.sql.sources.fastS3PartitionDiscovery.enabled": "false"
    }
}
]

```

7. Dans la section Mise en réseau, choisissez un cloud privé virtuel (VPC) et un sous-réseau situés sur votre rack. AWS Outposts Pour plus d'informations sur Amazon EMR sur Outposts, consultez [Clusters EMR sur AWS Outposts](#) dans le Guide de gestion Amazon EMR.
8. Dans la section Profil d'instance EC2 pour Amazon EMR, choisissez le rôle IAM auquel est jointe la [politique d'autorisation que vous avez créée précédemment](#).
9. Configurez les paramètres de cluster restants, puis choisissez Créer un cluster.

Présentation des configurations

Le tableau suivant décrit les configurations S3A et les valeurs à spécifier pour leurs paramètres lorsque vous configurez un cluster qui utilise S3 sur Outposts avec Amazon EMR.

Paramètre	Valeur par défaut	Valeur requise pour S3 sur Outposts	Explication
<code>fs.s3a.aws.credentials.provider</code>	Si la valeur n'est pas spécifiée, S3A recherchera S3 dans le compartiment de la région avec le nom de compartiment Outposts.	ARN du point d'accès du compartiment S3 sur Outposts	Amazon S3 sur Outposts prend en charge les points d'accès Virtual Private Cloud (VPC) uniquement comme seul moyen d'accéder à vos compartiments Outposts.
<code>fs.s3a.committer.name</code>	<code>file</code>	<code>magic</code>	Le validateur magique est le seul validateur pris en charge pour S3 sur Outposts.

Paramètre	Valeur par défaut	Valeur requise pour S3 sur Outposts	Explication
<code>fs.s3a.select.enabled</code>	TRUE	FALSE	S3 Select n'est pas pris en charge sur Outposts.
JAVA_HOME	<code>/usr/lib/jvm/java-8</code>	<code>/usr/lib/jvm/java-11-amazon-corretto.x86_64</code>	S3 sur Outposts sur S3A nécessite Java version 11.

Le tableau suivant décrit les configurations Spark et les valeurs à spécifier pour leurs paramètres lorsque vous configurez un cluster qui utilise S3 sur Outposts avec Amazon EMR.

Paramètre	Valeur par défaut	Valeur requise pour S3 sur Outposts	Explication
<code>spark.sql.sources.fastS3PartitionDiscovery.enabled</code>	TRUE	FALSE	S3 sur Outposts ne prend pas en charge la partition rapide.
<code>spark.executorEnv.JAVA_HOME</code>	<code>/usr/lib/jvm/java-8</code>	<code>/usr/lib/jvm/java-11-amazon-corretto.x86_64</code>	S3 sur Outposts sur S3A nécessite Java version 11.

Considérations

Tenez compte des points suivants lorsque vous intégrez Amazon EMR avec les compartiments S3 sur Outposts :

- Amazon S3 sur Outposts est pris en charge avec Amazon EMR version 7.0.0 et ultérieure.

- Le connecteur S3A est nécessaire pour utiliser S3 sur Outposts avec Amazon EMR. Seul S3A dispose des fonctionnalités requises pour interagir avec les compartiments S3 sur Outposts. Pour obtenir des informations sur la configuration du connecteur S3A, consultez [Conditions préalables](#).
- Amazon S3 sur Outposts prend en charge uniquement le chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3) avec Amazon EMR. Pour de plus amples informations, veuillez consulter [the section called “Chiffrement des données”](#).
- Amazon S3 on Outposts ne prend pas en charge les écritures avec le S3A. FileOutputCommittee Les écritures effectuées avec le S3A FileOutputCommittee sur les compartiments S3 on Outposts entraînent l'erreur suivante InvalidStorageClass: La classe de stockage que vous avez spécifiée n'est pas valide.
- Amazon S3 sur Outposts n'est pas pris en charge avec Amazon EMR sans serveur ni Amazon EMR sur EKS.
- Les journaux Amazon EMR sont stockés dans un emplacement Amazon S3 régional que vous sélectionnez et ne sont pas stockés localement dans le compartiment S3 sur Outposts.

Mise en cache d'autorisation et d'authentification

S3 sur Outposts met en cache de manière sécurisée les données d'authentification et d'autorisation localement sur les racks Outposts. Le cache supprime les allers-retours vers le parent Région AWS pour chaque demande. Cela élimine la variabilité introduite par les allers-retours réseau. Avec le cache d'authentification et d'autorisation dans S3 sur Outposts, vous obtenez des latences constantes indépendantes de la latence de la connexion entre les Outposts et la Région AWS.

Lorsque vous effectuez une demande d'API S3 sur Outposts, les données d'authentification et d'autorisation sont mises en cache de manière sécurisée. Les données mises en cache sont ensuite utilisées pour authentifier les demandes d'API d'objet S3 suivantes. S3 sur Outposts met en cache uniquement les données d'authentification et d'autorisation lorsque la demande est signée à l'aide de Signature Version 4A (SigV4A). Le cache est stocké localement sur les Outposts au sein du service S3 sur Outposts. Il est actualisé de manière asynchrone lorsque vous effectuez une demande d'API S3. Le cache est chiffré et aucune clé cryptographique en texte brut n'est stockée sur Outposts.

Le cache est valide pendant un maximum de 10 minutes lorsque l'Outpost est connecté à la Région AWS. Il est actualisé de manière asynchrone lorsque vous effectuez une demande d'API S3 sur Outposts, afin de garantir l'utilisation des politiques les plus récentes. Si l'Outpost est déconnecté de la Région AWS, le cache sera valide pendant 12 heures au maximum.

Configuration du cache d'autorisation et d'authentification

S3 sur Outposts met automatiquement en cache les données d'authentification et d'autorisation pour les demandes signées avec l'algorithme SigV4A. Pour plus d'informations, consultez [la section Signature des demandes d' AWS API](#) dans le guide de Gestion des identités et des accès AWS l'utilisateur. L'algorithme SigV4A est disponible dans les dernières versions du. AWS SDKs Vous pouvez l'obtenir via une dépendance aux [bibliothèques AWS CRT \(Common Runtime\)](#).

Vous devez utiliser la dernière version du AWS SDK et installer la dernière version du CRT. Par exemple, vous pouvez exécuter `pip install awscrt` pour obtenir la version la plus récente du CRT avec Boto3.

S3 sur Outposts ne met pas en cache les données d'authentification et d'autorisation pour les demandes signées avec l'algorithme SigV4.

Validation de la signature SigV4A

Vous pouvez l'utiliser AWS CloudTrail pour valider que les demandes ont été signées avec SIGv4a. Pour plus d'informations sur la configuration CloudTrail de S3 sur Outposts, consultez. [Surveillance de S3 sur les Outposts avec des logs AWS CloudTrail](#)

Après avoir configuré CloudTrail, vous pouvez vérifier comment une demande a été signée dans le SignatureVersion champ des CloudTrail journaux. Les demandes signées avec SigV4A ont un paramètre SignatureVersion défini sur AWS_4-ECDSA-P256-SHA256. Les demandes signées avec SigV4 ont un paramètre SignatureVersion défini sur AWS_4-HMAC-SHA256.

Sécurité dans S3 on Outposts

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 ceci comme la sécurité du cloud et la 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 programmes de [AWS conformité Programmes](#) de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à Amazon S3 on Outposts, consultez la section [AWS Services concernés par programme de conformitéAWS](#) .
- 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, ainsi que la législation et la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation de S3 on Outposts. Les rubriques suivantes vous montrent comment configurer S3 on Outposts pour répondre à vos objectifs de sécurité et de conformité. Vous apprendrez également à en utiliser d'autres Services AWS qui vous aideront à surveiller et à sécuriser vos ressources S3 on Outposts.

Rubriques

- [Configuration d'IAM avec S3 sur Outposts](#)
- [Chiffrement des données dans S3 sur Outposts](#)
- [AWS PrivateLink pour S3 sur Outposts](#)
- [AWS Clés de politique spécifiques à l'authentification Signature Version 4 \(SigV4\)](#)
- [AWS politiques gérées pour Amazon S3 sur Outposts](#)
- [Utilisation de rôles liés à un service pour Amazon S3 sur Outposts](#)

Configuration d'IAM avec S3 sur Outposts

Gestion des identités et des accès AWS (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent les personnes qui peuvent être authentifiées (connectées) et autorisées (disposant d'autorisations) pour utiliser des ressources Amazon S3 sur Outposts. IAM est un Service AWS que vous pouvez utiliser sans frais supplémentaires. Par défaut, les utilisateurs IAM ne disposent pas d'autorisations pour des ressources et des opérations S3 sur Outposts. Pour accorder des autorisations d'accès aux ressources et aux opérations d'API de S3 sur Outposts, vous pouvez utiliser IAM pour créer des [utilisateurs](#), [des groupes](#) ou [des rôles](#) et associer des autorisations.

Pour activer l'accès, ajoutez des autorisations à vos utilisateurs, groupes ou rôles :

- Utilisateurs et groupes dans AWS IAM Identity Center :

Créez un jeu 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 par un fournisseur d'identité :

Créez un rôle pour la fédération d'identité. Suivez les instructions de la rubrique [Création d'un rôle pour un fournisseur d'identité tiers \(fédération\)](#) dans le Guide de l'utilisateur IAM.

- Utilisateurs IAM :

- Créez un rôle que votre utilisateur peut assumer. Suivez les instructions de la rubrique [Création d'un rôle pour un utilisateur IAM](#) dans le Guide de l'utilisateur IAM.
- (Non recommandé) Attachez une politique directement à un utilisateur ou ajoutez un utilisateur à un groupe d'utilisateurs. Suivez les instructions de la rubrique [Ajout d'autorisations à un utilisateur \(console\)](#) du Guide de l'utilisateur IAM.

En plus des politiques basées sur l'identité d'IAM, S3 sur Outposts prend en charge les politiques de compartiment et de point d'accès. Les stratégies relatives aux compartiments et aux points d'accès sont des [stratégies basées sur les ressources](#) associées à la ressource S3 sur Outposts.

- Une politique de compartiment est attachée au compartiment et autorise ou refuse les requêtes adressées au compartiment et aux objets qu'il contient en fonction des éléments de la stratégie.
- En revanche, une stratégie de point d'accès est attachée au point d'accès et autorise ou refuse les requêtes adressées au point d'accès.

La stratégie de point d'accès fonctionne avec la politique de compartiment associée au compartiment S3 sur Outposts. Pour qu'une application ou un utilisateur puisse accéder à des objets dans un compartiment S3 sur Outposts via un point d'accès S3 sur Outposts, il faut que la politique de point d'accès et la politique de compartiment autorisent la demande.

Les restrictions que vous incluez dans une stratégie de point d'accès s'appliquent uniquement aux demandes effectuées via ce point d'accès. Par exemple, si un point d'accès est attaché à un compartiment, vous ne pouvez pas utiliser la politique de point d'accès pour autoriser ou refuser les demandes qui sont adressées directement au compartiment. Toutefois, les restrictions que vous imposez à une politique de compartiment peuvent autoriser ou refuser les requêtes adressées directement au compartiment ou via le point d'accès.

Dans une politique IAM ou une politique basée sur les ressources, vous définissez quelles actions S3 sur Outposts sont autorisées ou refusées. Les actions S3 sur Outposts correspondent à des opérations d'API S3 sur Outposts spécifiques. Les actions S3 sur Outposts utilisent le préfixe de l'espace de noms `s3-outposts:`. Les demandes adressées à l'API de contrôle S3 on Outposts dans un Région AWS et les demandes adressées aux points de terminaison de l'API d'objets sur l'Outpost sont authentifiées à l'aide d'IAM et autorisées par le biais du préfixe d'espace de noms `s3-outposts:`. Pour utiliser S3 sur Outposts, configurez vos utilisateurs IAM et autorisez-les par en fonction de l'espace de noms `s3-outposts:`.

Pour plus d'informations, consultez [Actions, ressources et clés de condition pour Amazon S3 sur Outposts](#) dans la Référence de l'autorisation de service.

Note

- Les listes de contrôle d'accès (ACLs) ne sont pas prises en charge par S3 sur Outposts.
- S3 sur Outposts considère par défaut le propriétaire du compartiment en tant que propriétaire d'objet, afin de s'assurer que le propriétaire d'un compartiment ne peut pas être empêché d'accéder ou de supprimer des objets.
- Le blocage de l'accès public S3 est toujours activé pour S3 sur Outposts afin de garantir que les objets ne peuvent jamais avoir un accès public.

Pour plus d'informations sur la configuration d'IAM pour S3 sur Outposts, consultez les rubriques suivantes.

Rubriques

- [Principes des politiques S3 sur Outposts](#)
- [Ressource ARNs pour S3 sur les Outposts](#)
- [Exemples de stratégies pour S3 sur Outposts](#)
- [Autorisations pour les points de terminaison S3 sur Outposts](#)
- [Rôles lié à un service pour S3 sur Outposts](#)

Principes des politiques S3 sur Outposts

Lorsque vous créez une stratégie basée sur les ressources pour accorder l'accès à votre compartiment S3 sur Outposts, vous devez utiliser l'élément `Principal` pour spécifier la personne ou application qui peut effectuer une requête d'action ou d'opération sur cette ressource. Pour les stratégies S3 sur Outposts, vous pouvez utiliser l'un des principes suivants :

- Un Compte AWS
- Un utilisateur IAM
- Un rôle IAM
- Tous les principaux, en utilisant un caractère générique (*) dans une politique qui utilise un élément `Condition` pour limiter l'accès à une plage d'adresses IP spécifique

Important

Vous ne pouvez pas écrire de politique pour un compartiment S3 sur Outposts qui utilise un caractère générique (*) dans l'élément `Principal`, sauf si la politique inclut également un élément `Condition` qui restreint l'accès à une plage d'adresses IP spécifique. Cette restriction garantit qu'il n'y a pas d'accès public à votre compartiment S3 sur Outposts. Pour obtenir un exemple, consultez [Exemples de stratégies pour S3 sur Outposts](#).

Pour en savoir plus sur l'élément `Principal`, consultez [AWS JSON policy elements: Principal](#) (Élément de stratégie JSON : Principe) dans le Guide de l'utilisateur IAM.

Ressource ARNs pour S3 sur les Outposts

Les Amazon Resource Names (ARNs) pour S3 on Outposts contiennent l'ID de l'Outpost en plus de l' Région AWS adresse d'accueil de l'Outpost, de l' Compte AWS ID et du nom de la ressource. Pour

accéder à vos compartiments et à vos objets Outposts et y effectuer des actions, vous devez utiliser l'un des formats ARN présentés dans le tableau suivant.

La *partition* valeur de l'ARN fait référence à un groupe de Régions AWS. Chacune Compte AWS est limitée à une partition. Les partitions prises en charge sont les suivantes :

- aws – Régions AWS
- aws-us-gov— AWS GovCloud (US) Régions

Le tableau suivant présente les formats d'ARN pour S3 sur Outposts.

ARN pour Amazon S3 sur Outposts	Format ARN	Exemple
ARN de compartiment	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i> / bucket/ <i>bucket_name</i>	arn:aws:s3-outposts: <i>us-west-2</i> :123456789012 :outpost/ <i>op-01ac5d28a6a232904</i> / bucket/ <i>amzn-s3-demo-bucket1</i>
ARN de point d'accès	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i> /accesspoint/ <i>accesspoint_name</i>	arn:aws:s3-outposts: <i>us-west-2</i> :123456789012 :outpost/ <i>op-01ac5d28a6a232904</i> /accesspoint/ <i>access-point-name</i>
ARN d'objet	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i> / bucket/ <i>bucket_name</i> / object/ <i>object_key</i>	arn:aws:s3-outposts: <i>us-west-2</i> :123456789012 :outpost/ <i>op-01ac5d28a6a232904</i> / bucket/ <i>amzn-s3-demo-</i>

ARN pour Amazon S3 sur Outposts	Format ARN	Exemple
		<i>bucket1 /object/myobject</i>
ARN d'objet de point d'accès S3 sur Outposts (utilisé dans les politiques)	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i> /accesspoint/ <i>accesspoint_name</i> / object/ <i>object_key</i>	arn:aws:s3-outposts: <i>us-west-2</i> : <i>123456789012</i> :outpost/ <i>op-01ac5d28a6a232904</i> /accesspoint/ <i>access-point-name/object/myobject</i>
ARN pour S3 sur Outposts	arn: <i>partition</i> :s3-outposts: <i>region</i> : <i>account_id</i> :outpost / <i>outpost_id</i>	arn:aws:s3-outposts: <i>us-west-2</i> : <i>123456789012</i> :outpost/ <i>op-01ac5d28a6a232904</i>

Exemples de stratégies pour S3 sur Outposts

Exemple: politique de compartiment S3 on Outposts avec un principal Compte AWS


La politique de compartiment suivante utilise un Compte AWS principal pour accorder l'accès à un compartiment S3 on Outposts. Pour utiliser cette politique de compartiment, remplacez *user input placeholders* par vos propres informations.

Exemple: politique de compartiment S3 sur Outposts avec principal générique (*) et clé de condition pour limiter l'accès à une plage d'adresses IP spécifique

La politique de compartiment suivante utilise un principal générique (*) avec la condition `aws:SourceIp` pour limiter l'accès à une plage d'adresses IP spécifique. Pour utiliser cette politique de compartiment, remplacez *user input placeholders* par vos propres informations.

Autorisations pour les points de terminaison S3 sur Outposts

S3 sur Outposts nécessite ses propres autorisations dans IAM pour gérer les actions des points de terminaison de S3 sur Outposts.

 Note

- Pour les points de terminaison qui utilisent le type d'accès du groupe d'adresses IP clients (groupe CoIP), vous devez également disposer des autorisations pour travailler avec des adresses IP à partir de votre groupe CoIP, comme décrit dans le tableau suivant.
- Pour les comptes partagés qui accèdent à S3 sur Outposts en utilisant AWS Resource Access Manager, les utilisateurs de ces comptes partagés ne peuvent pas créer leurs propres points de terminaison sur un sous-réseau partagé. Si un utilisateur d'un compte partagé souhaite gérer ses propres points de terminaison, le compte partagé doit créer son propre sous-réseau sur l'Outpost. Pour de plus amples informations, veuillez consulter [the section called "Partager S3 sur Outposts"](#).

Le tableau suivant présente les autorisations IAM liées aux points de terminaison S3 sur Outposts.

Action	Autorisations IAM
CreateEndpoint	s3-outposts:CreateEndpoint ec2:CreateNetworkInterface ec2:DescribeNetworkInterfaces ec2:DescribeVpcs ec2:DescribeSecurityGroups ec2:DescribeSubnets ec2:CreateTags iam:CreateServiceLinkedRole Pour les points de terminaison qui utilisent le type d'accès du groupe d'adresses IP

Action	Autorisations IAM
	<p>clients (groupe CoIP) sur site, les autorisations supplémentaires suivantes sont requises :</p> <p><code>s3-outposts:CreateEndpoint</code></p> <p><code>ec2:DescribeCoipPools</code></p> <p><code>ec2:GetCoipPoolUsage</code></p> <p><code>ec2:AllocateAddress</code></p> <p><code>ec2:AssociateAddress</code></p> <p><code>ec2:DescribeAddresses</code></p> <p><code>ec2:DescribeLocalGatewayRouteTableVpcAssociations</code></p>
DeleteEndpoint	<p><code>s3-outposts>DeleteEndpoint</code></p> <p><code>ec2>DeleteNetworkInterface</code></p> <p><code>ec2:DescribeNetworkInterfaces</code></p> <p>Pour les points de terminaison qui utilisent le type d'accès du groupe d'adresses IP clients (groupe CoIP) sur site, les autorisations supplémentaires suivantes sont requises :</p> <p><code>s3-outposts>DeleteEndpoint</code></p> <p><code>ec2:DisassociateAddress</code></p> <p><code>ec2:DescribeAddresses</code></p> <p><code>ec2:ReleaseAddress</code></p>
ListEndpoints	<code>s3-outposts:ListEndpoints</code>

Note

Vous pouvez utiliser des balises de ressources dans une politique IAM pour gérer les autorisations.

Rôles lié à un service pour S3 sur Outposts

S3 sur Outposts utilise des rôles liés à un service IAM pour créer des ressources réseau en votre nom. Pour de plus amples informations, veuillez consulter [Utilisation de rôles liés à un service pour Amazon S3 sur Outposts](#).

Chiffrement des données dans S3 sur Outposts

Par défaut, toutes les données stockées dans Amazon S3 sur Outposts sont chiffrées à l'aide du chiffrement côté serveur avec les clés de chiffrement gérées Amazon S3 (SSE-S3). Pour plus d'informations, consultez [Utilisation du chiffrement côté serveur avec des clés gérées par Amazon S3 \(SSE-S3\)](#) dans le Guide de l'utilisateur Amazon S3.

Vous pouvez éventuellement utiliser le chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C). Pour utiliser SSE-C, spécifiez une clé de chiffrement dans le cadre de vos demandes d'API sur les objets. Un chiffrement côté serveur chiffre uniquement les données d'objet, pas les métadonnées d'objet. Pour plus d'informations, consultez [Utilisation du chiffrement côté serveur avec les clés fournies par le client](#) dans le Guide de l'utilisateur Amazon S3.

Note

S3 on Outposts ne prend pas en charge le chiffrement côté serveur avec les clés AWS Key Management Service (AWS KMS) (SSE-KMS).

AWS PrivateLink pour S3 sur Outposts

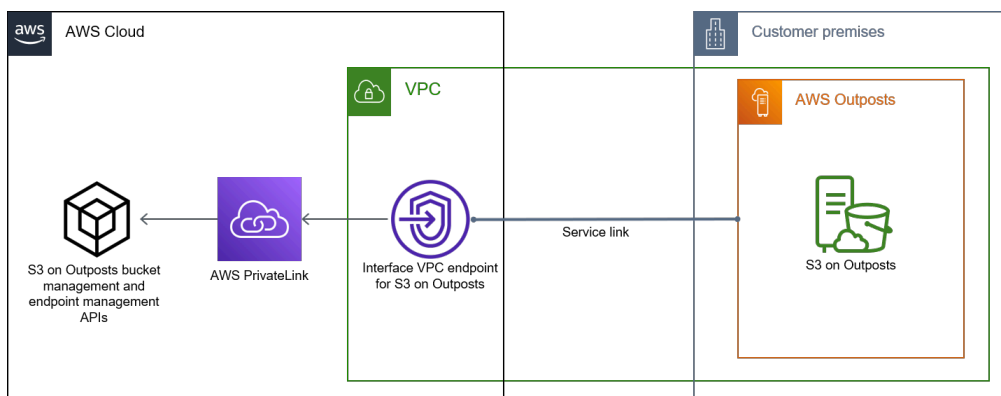
S3 on Outposts prend en charge AWS PrivateLink, ce qui fournit un accès de gestion direct à votre stockage S3 on Outposts via un point de terminaison privé au sein de votre réseau privé virtuel. Cela vous permet de simplifier l'architecture de votre réseau interne et d'effectuer des opérations de gestion sur votre stockage d'objets Outposts en utilisant des adresses IP privées dans votre cloud

privé virtuel (VPC). L'utilisation AWS PrivateLink élimine le besoin d'utiliser des adresses IP publiques ou des serveurs proxy.

[Avec AWS PrivateLink Amazon S3 on Outposts, vous pouvez configurer des points de terminaison VPC d'interface dans votre cloud privé virtuel \(VPC\) pour accéder à la gestion de votre bucket S3 on Outposts et à la gestion des points de terminaison.](#) APIs Les points de terminaison d'un VPC d'interface sont directement accessibles depuis des applications déployées dans votre VPC ou sur site par l'intermédiaire de votre réseau privé virtuel (VPN) ou d' AWS Direct Connect. Vous pouvez accéder à la gestion des compartiments et des terminaux APIs via AWS PrivateLink. AWS PrivateLink ne prend pas en charge [les opérations d'API de transfert de données](#), telles que GET, PUT, APIs etc. Ces opérations sont déjà transférées en privé via la configuration du point de terminaison et du point d'accès S3 sur Outposts. Pour de plus amples informations, veuillez consulter [Mise en réseau pour S3 on Outposts](#).

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 aux points de terminaison d'interface pour S3 on Outposts sont automatiquement acheminées vers le bucket S3 on Outposts et la gestion des points de terminaison sur le réseau. APIs AWS 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 ().Site-to-Site VPN Pour plus d'informations sur la façon de connecter votre VPC à votre réseau sur site, consultez le [Guide de l'utilisateur Direct Connect](#) et le [Guide de l'utilisateur AWS Site-to-Site VPN](#).

Les points de terminaison de l'interface acheminent les demandes pour S3 sur le bucket Outposts et la APIs gestion des points de terminaison via AWS le réseau et AWS PrivateLink via le réseau, comme illustré dans le schéma suivant.



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

- [Restrictions et limitations](#)
- [Accès aux points de terminaison d'interface S3 sur Outposts](#)
- [Mise à jour d'une configuration DNS sur site](#)
- [Création d'un point de terminaison de VPC pour S3 sur Outposts](#)
- [Création de stratégies de compartiment et de stratégies de point de terminaison de VPC pour S3 sur Outposts](#)

Restrictions et limitations

Lorsque vous accédez à S3 on Outposts APIs via la gestion du bucket et des endpoints, les limites du AWS PrivateLink VPC s'appliquent. Pour plus d'informations, consultez les sections [Propriétés et limitations des points de terminaison d'interface](#) et [Quotas AWS PrivateLink](#) du Guide AWS PrivateLink .

En outre, AWS PrivateLink ne prend pas en charge les éléments suivants :

- [Points de terminaison FIPS \(Federal Information Processing Standard\)](#)
- [Transfert de données S3 on Outposts](#), par exemple APIs, GET, PUT et opérations d'API d'objets similaires.
- DNS privé

Accès aux points de terminaison d'interface S3 sur Outposts

Pour accéder au bucket S3 on Outposts et à l' APIs aide de la gestion des terminaux AWS PrivateLink, vous devez mettre à jour vos applications afin d'utiliser des noms DNS spécifiques aux points de terminaison. Lorsque vous créez un point de terminaison d'interface, deux types de S3 spécifiques au point de terminaison sont AWS PrivateLink générés sous les noms d'Outposts : régional et zonal.

- Noms DNS régionaux : incluez un ID de point de terminaison VPC unique, un identifiant de service, le Région AWS, etvpce . amazonaws . com, par exemple, . *vpce-1a2b3c4d-5e6f* . s3-outposts . us-east-1 . vpce . amazonaws . com
- Noms DNS zonaux : incluez un ID de point de terminaison VPC unique, la zone de disponibilité, un identifiant de service, Région AWS le, vpce . amazonaws . com et, par exemple, .

vpce-1a2b3c4d-5e6f-us-east-1.s3-outposts.us-east-1.vpce.amazonaws.com

Vous pouvez utiliser cette option si votre architecture isole les zones de disponibilité. Par exemple, vous pouvez utiliser des noms DNS de zone pour contenir les pannes ou réduire les coûts de transfert de données de région.

Important

Les points de terminaison de l'interface S3 sur Outposts sont résolus depuis le domaine DNS public. S3 sur Outposts ne prend pas en charge le DNS privé. Utilisez le `--endpoint-url` paramètre pour la gestion de l'ensemble des compartiments et des terminaux APIs.

AWS CLI exemples

Utilisez les `--endpoint-url` paramètres `--region` et pour accéder à la gestion des compartiments et à la gestion des terminaux APIs via les points de terminaison de l'interface S3 on Outposts.

Exemple: utiliser l'URL du point de terminaison pour répertorier les compartiments avec l'API de contrôle S3

Dans l'exemple suivant, remplacez la région *us-east-1*, l'URL de point de terminaison de VPC *vpce-1a2b3c4d-5e6f.s3.us-east-1.vpce.amazonaws.com* et l'ID du compte *111122223333* par les informations appropriées.

```
aws s3control list-regional-buckets --region us-east-1 --endpoint-url
  https://vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com --account-
  id 111122223333
```

AWS Exemples de SDK

Passez SDKs à la dernière version et configurez vos clients pour qu'ils utilisent une URL de point de terminaison pour accéder à l'API de contrôle S3 pour les points de terminaison de l'interface Outposts.

SDK for Python (Boto3)

Exemple: utiliser une URL de point de terminaison pour accéder à l'API de contrôle S3

Dans l'exemple suivant, remplacez la région *us-east-1* et l'ID du point de terminaison de VPC *vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com* par des informations appropriées.

```
control_client = session.client(
    service_name='s3control',
    region_name='us-east-1',
    endpoint_url='https://vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com'
)
```

Pour plus d'informations, consultez [AWS PrivateLink for Amazon S3](#) (pour Amazon S3) dans le Guide du développeur Boto3.

SDK for Java 2.x

Exemple: utiliser une URL de point de terminaison pour accéder à l'API de contrôle S3

Dans l'exemple suivant, remplacez l'URL de point de terminaison de VPC *vpce-1a2b3c4d-5e6f.s3-outposts.us-east-1.vpce.amazonaws.com* et la région *Region.US_EAST_1* par des informations appropriées.

```
// control client
Region region = Region.US_EAST_1;
S3ControlClient = S3ControlClient.builder().region(region)

    .endpointOverride(URI.create("https://vpce-1a2b3c4d-5e6f.s3-outposts.us-
east-1.vpce.amazonaws.com"))
    .build()
```

Pour plus d'informations, consultez [S3ControlClient](#) dans la Référence d'API AWS SDK pour Java .

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 de l'interface pour la gestion des compartiments et des points de terminaison S3 on Outposts APIs, vous n'avez pas besoin de mettre à jour votre résolveur DNS local. 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 S3 sur Outposts.

Création d'un point de terminaison de VPC pour S3 sur Outposts

Pour créer un point de terminaison d'interface de VPC pour S3 sur Outposts, consultez [Création d'un point de terminaison de VPC](#) dans le Guide AWS PrivateLink .

Création de stratégies de compartiment et de stratégies de point de terminaison de VPC pour S3 sur Outposts

Vous pouvez attacher une stratégie de point de terminaison à votre point de terminaison de VPC qui contrôle l'accès à S3 sur Outposts. Vous pouvez également utiliser la condition `aws:sourceVpce` dans les stratégies de compartiment S3 sur Outposts pour restreindre l'accès à des compartiments spécifiques depuis un point de terminaison de VPC spécifique. Grâce aux politiques des points de terminaison VPC, vous pouvez contrôler l'accès à S3 sur la gestion APIs des compartiments et des points de terminaison d'Outposts. APIs Grâce aux politiques relatives aux compartiments, vous pouvez contrôler l'accès au S3 sur la gestion des compartiments Outposts. APIs Toutefois, vous ne pouvez pas gérer l'accès aux actions d'objet pour S3 sur Outposts à l'aide de `aws:sourceVpce`.

Les stratégies d'accès pour S3 sur Outposts spécifient les informations suivantes :

- Le principal Gestion des identités et des accès AWS (IAM) pour lequel les actions sont autorisées ou refusées.
- Les actions de contrôle S3 qui sont autorisées ou refusées.
- Les ressources S3 sur Outposts pour lesquelles des actions sont autorisées ou refusées.

Les exemples suivants montrent les stratégies qui restreignent l'accès à un compartiment ou à un point de terminaison. 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](#).

Important

- Lors de l'application des exemples de stratégie pour les points de terminaison de VPC décrits dans cette section, vous pouvez bloquer involontairement votre accès au compartiment. Les autorisations attribuées à un compartiment qui restreignent 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 politique de compartiment suivant, remplacez l'ID de point de terminaison de VPC par une valeur appropriée pour votre cas d'utilisation. Dans le cas contraire, vous ne parviendrez pas à accéder à votre compartiment.
- Si votre stratégie n'autorise l'accès à un compartiment S3 sur Outposts qu'à partir d'un point de terminaison de VPC spécifique, elle désactive l'accès à la console pour ce compartiment car les demandes de console ne proviennent pas du point de terminaison de VPC spécifié.

Rubriques

- [Exemple : restriction de l'accès à un compartiment spécifique depuis le point de terminaison d'un VPC](#)
- [Exemple : refus d'accès depuis un point de terminaison de VPC spécifique dans une politique de compartiment S3 sur Outposts](#)

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 S3 sur Outposts spécifiques uniquement. La politique suivante restreint l'accès à l' `GetBucketPolicy` action uniquement au *exemple-outpost-bucket*. Pour utiliser cette stratégie, remplacez les exemples de valeur par vos propres valeurs.

JSON

```
{
  "Version": "2012-10-17",
  "Id": "Policy1415115909151",
  "Statement": [
    {
      "Sid": "Access-to-specific-bucket-only",
      "Principal": {
```

```

        "AWS": "111122223333"
    },
    "Action": "s3-outposts:GetBucketPolicy",
    "Effect": "Allow",
    "Resource": "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket"
    }
]
}

```

Exemple : refus d'accès depuis un point de terminaison de VPC spécifique dans une politique de compartiment S3 sur Outposts

La politique de compartiment S3 on Outposts suivante refuse l'accès au *example-outpost-bucket* compartiment via GetBucketPolicy le point de terminaison VPC. *vpce-1a2b3c4d*

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 de VPC, mais uniquement l'ID du point de terminaison. Pour utiliser cette stratégie, remplacez les exemples de valeur par vos propres valeurs.

JSON

```

{
  "Version": "2012-10-17",
  "Id": "Policy1415115909152",
  "Statement": [
    {
      "Sid": "Deny-access-to-specific-VPCE",
      "Principal": {
        "AWS": "111122223333"
      },
      "Action": "s3-outposts:GetBucketPolicy",
      "Effect": "Deny",
      "Resource": "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket",
      "Condition": {
        "StringEquals": {
          "aws:sourceVpce": "vpce-1a2b3c4d"
        }
      }
    }
  ]
}

```

```

    ]
}

```

AWS Clés de politique spécifiques à l'authentification Signature Version 4 (SigV4)

Le tableau suivant indique les clés de condition liées à l'authentification AWS Signature Version 4 (Sigv4) que vous pouvez utiliser avec Amazon S3 sur Outposts. Dans une stratégie de compartiment, vous pouvez ajouter ces conditions pour imposer un comportement spécifique lorsque les requêtes sont authentifiées en utilisant Signature Version 4. Pour obtenir des exemples de politiques, consultez [Exemples de stratégies de compartiment qui utilisent des clés de condition associées à Signature Version 4](#). Pour plus d'informations sur l'authentification des demandes à l'aide de Signature version 4, consultez [Authentification des demandes \(AWS Signature version 4\)](#) dans le manuel Amazon Simple Storage Service API Reference

Clés applicables	Description
s3-outposts:authType	<p>S3 on Outposts prend en charge différentes méthodes d'authentification. Pour limiter les requêtes entrantes afin d'utiliser d'une méthode d'authentification spécifique, vous pouvez utiliser cette clé de condition facultative. Par exemple, vous pouvez utiliser cette clé de condition pour autoriser uniquement l'en-tête <code>HTTPAuthorization</code> pour l'authentification de la demande.</p> <p>Valeurs valides :</p> <p>REST-HEADER</p> <p>REST-QUERY-STRING</p>
s3-outposts:signatureAge	<p>La durée, en millisecondes, pendant laquelle une signature est valide dans une demande authentifiée.</p> <p>Cette condition ne fonctionne que pour les versions présignées URLs.</p> <p>Dans Signature Version 4, la clé de signature est valide pendant sept jours au maximum. Par conséquent, les signatures ne restent</p>

Clés applicables	Description
<p>s3-outposts:x-amz-content-sha256</p>	<p>valides que pendant sept jours. Pour plus d'informations, consultez Introduction à la signature des demandes dans la Référence d'API Amazon Simple Storage Service. Vous pouvez utiliser cette condition pour limiter davantage la durée de la signature.</p> <p>Exemple de valeur : 600000</p> <p>Vous pouvez utiliser cette clé de condition pour interdire les contenus non signés dans votre compartiment.</p> <p>Lorsque vous utilisez Signature Version 4, pour les requêtes qui utilisent l'en-tête <code>Authorization</code>, vous ajoutez l'en-tête <code>x-amz-content-sha256</code> dans le calcul de signature, puis définissez sa valeur sur la charge utile du hachage.</p> <p>Vous pouvez utiliser cette clé de condition dans votre stratégie de compartiment pour refuser tous les chargements où les charges utiles ne sont pas signées. Par exemple :</p> <ul style="list-style-type: none"> • Refuser les chargements qui utilisent l'en-tête <code>Authorization</code> pour authentifier les requêtes mais ne signent pas la charge utile. Pour plus d'informations, consultez Transfert de la charge utile en un seul fragment dans la Référence d'API Amazon Simple Storage Service. • Refusez les téléchargements utilisant le URLs présigné. Les présignés ont URLs toujours <code>UNSIGNED_PAYLOAD</code>. Pour plus d'informations, consultez Demandes d'authentification et Méthodes d'authentification dans la Référence des API Amazon Simple Storage Service. <p>Valeur valide : UNSIGNED-PAYLOAD</p>

Exemples de stratégies de compartiment qui utilisent des clés de condition associées à Signature Version 4

Pour utiliser les exemples suivants, remplacez *user input placeholders* par vos propres informations.

Exemple: s3-outposts:signatureAge

La stratégie de compartiment suivante refuse toute demande d'URL présignée S3 on Outposts sur les objets dans `example-outpost-bucket` si la signature date de plus de 10 minutes.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Deny a presigned URL request if the signature is more than 10
minutes old",
      "Effect": "Deny",
      "Principal": {"AWS": "444455556666"},
      "Action": "s3-outposts:*",
      "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
      "Condition": {
        "NumericGreaterThan": {"s3-outposts:signatureAge": 600000},
        "StringEquals": {"s3-outposts:authType": "REST-QUERY-STRING"}
      }
    }
  ]
}
```

Exemple: s3-outposts:authType

La stratégie de compartiment suivante autorise uniquement les requêtes qui utilisent l'en-tête `Authorization` pour l'authentification des demandes. Toutes les demandes d'URL présignées seront refusées car les URL présignées utilisent des paramètres de requête pour fournir des informations de demande et d'authentification. Pour de plus amples informations, veuillez consulter [Authentication methods](#) (Méthodes d'authentification dans la Référence d'API Amazon Simple Storage Service).

JSON

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

```

"Statement": [
  {
    "Sid": "Allow only requests that use the Authorization header for
request authentication. Deny presigned URL requests.",
    "Effect": "Deny",
    "Principal": {"AWS": "111122223333"},
    "Action": "s3-outposts:*",
    "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
    "Condition": {
      "StringNotEquals": {
        "s3-outposts:authType": "REST-HEADER"
      }
    }
  }
]
}

```

Example: s3-outposts:x-amz-content-sha256

La politique de compartiment suivante interdit tout téléchargement contenant des charges utiles non signées, tel que les téléchargements utilisant le présigné. URLs Pour de plus amples informations, veuillez consulter [Authenticating requests](#) (Requêtes d'authentification) et [Authentication methods](#) (Méthodes d'authentification dans la Référence d'API Amazon Simple Storage Service).

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Deny uploads with unsigned payloads.",
      "Effect": "Deny",
      "Principal": {"AWS": "111122223333"},
      "Action": "s3-outposts:*",
      "Resource": "arn:aws:s3-outposts:us-
east-1:111122223333:outpost/op-01ac5d28a6a232904/bucket/example-outpost-bucket/
object/*",
      "Condition": {
        "StringEquals": {

```

```
    "s3-outposts:x-amz-content-sha256": "UNSIGNED-PAYLOAD"
  }
}
]
```

AWS politiques gérées pour Amazon S3 sur Outposts

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 : AWSS3 OnOutpostsServiceRolePolicy

Gère les ressources réseau à votre place dans le cadre du rôle lié à un service AWSServiceRoleForS3OnOutposts.

Pour consulter les autorisations associées à cette politique, consultez [AWSS3OnOutpostsServiceRolePolicy](#).

S3 on Outposts met à jour les politiques gérées AWS

Consultez les détails des mises à jour des politiques AWS gérées pour S3 sur Outposts depuis que ce service a commencé à suivre ces modifications.

Modifier	Description	Date
Ajout de <code>AWSS3OnOutpostsServiceRolePolicy</code> dans S3 sur Outposts	S3 sur Outposts a ajouté <code>AWSS3OnOutpostsServiceRolePolicy</code> en tant que partie intégrante du rôle lié à un service <code>AWSServiceRoleForS3OnOutposts</code> , qui gère les ressources réseau à votre place.	3 octobre 2023
Introduction du suivi des modifications dans S3 sur Outposts	S3 on Outposts a commencé à suivre les modifications apportées à ses politiques AWS gérées.	3 octobre 2023

Utilisation de rôles liés à un service pour Amazon S3 sur Outposts

[Amazon S3 on Outposts utilise des rôles liés à un Gestion des identités et des accès AWS service \(IAM\)](#). Un rôle lié à un service est un type unique de rôle IAM lié directement à S3 sur Outposts. Les rôles liés à un service sont prédéfinis par S3 sur Outposts et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service simplifie la configuration de S3 sur Outposts, car vous n'avez pas besoin d'ajouter manuellement les autorisations nécessaires. S3 sur Outposts définit les autorisations de ses rôles liés à un service ; sauf définition contraire, seul S3 sur Outposts peut endosser ses rôles. Les autorisations définies comprennent la politique de confiance et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Vos ressources S3 sur Outposts sont ainsi protégées, puisque vous ne pouvez pas supprimer accidentellement l'autorisation d'accéder aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez la section [AWS Services qui fonctionnent avec IAM](#) et recherchez les services dont la valeur est Oui dans la colonne Rôles liés aux services. Sélectionnez un Oui ayant un lien pour consulter la documentation du rôle lié à un service, pour ce service.

Autorisations de rôle lié à un service pour S3 sur Outposts

S3 on Outposts utilise le rôle lié à un service nommé `AWSServiceRoleForS3 OnOutposts` pour vous aider à gérer les ressources réseau.

Le rôle lié à un service `AWSServiceRoleForS3OnOutposts` approuve les services suivants pour endosser le rôle :

- `s3-outposts.amazonaws.com`

La politique d'autorisations de rôle nommée `AWSS3OnOutpostsServiceRolePolicy` permet à S3 sur Outposts d'effectuer les actions suivantes sur les ressources spécifiées :

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcs",
        "ec2:DescribeCoipPools",
        "ec2:GetCoipPoolUsage",
        "ec2:DescribeAddresses",
        "ec2:DescribeLocalGatewayRouteTableVpcAssociations"
      ],
      "Resource": "*",
      "Sid": "DescribeVpcResources"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateNetworkInterface"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:security-group/*"
      ],
    }
  ]
}
```

```

    "Sid": "CreateNetworkInterface"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateNetworkInterface"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/CreatedBy": "S3 On Outposts"
      }
    },
    "Sid": "CreateTagsForCreateNetworkInterface"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:AllocateAddress"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:ipv4pool-ec2/*"
    ],
    "Sid": "AllocateIpAddress"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:AllocateAddress"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:elastic-ip/*"
    ],
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/CreatedBy": "S3 On Outposts"
      }
    },
    "Sid": "CreateTagsForAllocateIpAddress"
  },
  {
    "Effect": "Allow",

```

```

    "Action": [
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:CreateNetworkInterfacePermission",
      "ec2>DeleteNetworkInterface",
      "ec2>DeleteNetworkInterfacePermission",
      "ec2:DisassociateAddress",
      "ec2:ReleaseAddress",
      "ec2:AssociateAddress"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/CreatedBy": "S3 On Outposts"
      }
    },
    "Sid": "ReleaseVpcResources"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": [
          "CreateNetworkInterface",
          "AllocateAddress"
        ],
        "aws:RequestTag/CreatedBy": [
          "S3 On Outposts"
        ]
      }
    },
    "Sid": "CreateTags"
  }
]
}

```

Vous devez configurer des autorisations pour permettre à une entité IAM (comme 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 sur Outposts

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un point de terminaison S3 on Outposts dans l' AWS Management Console AWS API AWS CLI, S3 on Outposts crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un point de terminaison S3 sur Outposts, S3 sur Outposts recrée automatiquement le rôle lié à un service.

Vous pouvez également utiliser la console IAM pour créer un rôle lié à un service avec le cas d'utilisation S3 sur Outposts. Dans l'API AWS CLI ou dans l' AWS API, créez un rôle lié à un service avec le nom du `s3-outposts.amazonaws.com` service. Pour plus d'informations, consultez [Création d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM. Si vous supprimez ce rôle lié à un service, vous pouvez utiliser ce même processus pour créer le rôle à nouveau.

Modification d'un rôle lié à un service pour S3 sur Outposts

S3 sur Outposts ne vous permet pas de modifier le rôle lié à un service `AWSServiceRoleForS3onOutposts`. Cela concerne également le nom du rôle, car diverses entités peuvent y faire référence. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez [Modification d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Suppression d'un rôle lié à un service pour S3 sur Outposts

Si vous n'avez plus besoin d'utiliser une fonctionnalité ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, vous n'avez aucune entité inutilisée qui n'est pas surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

Note

Si le service S3 sur Outposts utilise le rôle pendant que vous tentez de supprimer les ressources, la suppression peut échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les ressources S3 on Outposts utilisées par le AWSService RoleFor rôle S3 OnOutposts

1. [Supprimez les points de terminaison S3 on Outposts](#) dans votre Compte AWS ensemble.
Régions AWS
2. Supprimez le rôle lié à un service à l'aide d'IAM.

Utilisez la console IAM, le AWS CLI, ou l' AWS API pour supprimer le rôle lié au `AWSServiceRoleForS3OnOutposts` service. Pour plus d'informations, consultez la section [Suppression d'un rôle lié à un service](#) dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés à un service S3 sur Outposts

S3 on Outposts permet d'utiliser des rôles liés à un service partout Régions AWS où le service est disponible. Pour en savoir plus, consultez [Régions et points de terminaison S3 sur Outposts](#).

Gestion de stockage S3 on Outposts

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur APIs les compartiments Outpost que sur les compartiments 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 Command Line Interface (AWS CLI) ou REST. AWS SDKs Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Pour plus d'informations sur la gestion et le partage de votre capacité de stockage Amazon S3 sur Outposts, consultez les rubriques suivantes.

Rubriques

- [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#)
- [Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts](#)
- [Répliquer des objets pour S3 sur Outposts](#)
- [Partage de S3 sur Outposts à l'aide de AWS RAM](#)
- [Autres Services AWS qui utilisent S3 sur Outposts](#)

Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts

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.

Les compartiments Amazon S3 sur Outposts ont trois états de gestion des versions :

- **Non versionné** : si vous n'avez jamais activé ou suspendu la gestion des versions S3 sur votre compartiment, celle-ci est non versionnée et ne renvoie aucun statut de gestion des versions S3. Pour plus d'informations sur la gestion des versions S3, consultez [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#).
- **Activé** : active la gestion des versions S3 pour les objets du compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. 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, par exemple [PutObject](#), les nouveaux objets obtiennent un ID de version unique.
- **Suspendu** : active la gestion des versions S3 pour les objets du compartiment. Tous les objets ajoutés au compartiment après que la gestion des versions ait été suspendue reçoivent l'ID de version null. Pour plus d'informations, consultez [Ajout d'objets dans des compartiments désactivés pour la gestion des versions](#) dans le Guide de l'utilisateur Amazon S3.

Lorsque vous activez la gestion des versions S3 pour un compartiment S3 sur Outposts, il ne peut jamais revenir à un état non versionné. Toutefois, vous pouvez suspendre la gestion des versions. Pour plus d'informations sur la gestion des versions S3, consultez [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#).

Pour chaque objet de votre compartiment, vous avez une version actuelle et zéro, une ou plusieurs versions anciennes. Pour réduire les coûts de stockage, vous pouvez configurer les règles de cycle de vie de votre compartiment S3 de manière à ce que les versions anciennes expirent après une durée spécifiée. Pour de plus amples informations, veuillez consulter [Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts](#).

Les exemples suivants vous montrent comment activer ou suspendre le contrôle de version pour un bucket S3 on Outposts existant à l'aide de and AWS Management Console AWS Command Line Interface the AWS CLI(). Pour créer un compartiment avec la gestion des versions S3 activée, consultez [Création d'un compartiment S3 sur Outposts](#).

Note

Celui Compte AWS qui crée le bucket en est propriétaire et est le seul à pouvoir y effectuer des actions. Les compartiments possèdent des propriétés de configuration telles que Outpost, balise, chiffrement par défaut et paramètres de point d'accès. Les paramètres du point d'accès comprennent le cloud privé virtuel (VPC), la stratégie du point d'accès

pour accéder aux objets du compartiment et d'autres métadonnées. Pour de plus amples informations, veuillez consulter [Spécifications de S3 on Outposts](#).

Utilisation de la console S3

Modifier les paramètres de la gestion des versions 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 Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts pour lequel vous voulez activer la gestion des versions S3.
4. Choisissez l'onglet Propriétés.
5. Sous Bucket Versioning (Gestion des versions de compartiment), choisissez Edit (Modifier).
6. Modifiez les paramètres de gestion des versions S3 pour le compartiment en choisissant l'une des options suivantes :
 - Pour suspendre la gestion des versions S3 et arrêter la création de nouvelles versions d'objets, choisissez Suspend (Suspendre).
 - Pour activer la gestion des versions S3 et enregistrer plusieurs copies distinctes de chaque objet, choisissez Enable (Activer).
7. Sélectionnez Enregistrer les modifications.

En utilisant le AWS CLI

Pour activer ou suspendre le versionnement S3 pour votre compartiment à l'aide de AWS CLI, utilisez la `put-bucket-versioning` commande, comme indiqué dans les exemples suivants. Pour utiliser ces exemples, remplacez chaque *user input placeholder* par vos propres informations.

Pour plus d'informations, consultez [put-bucket-versioning](#) dans la référence AWS CLI .

Exemple: Activer la gestion des versions S3

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket --versioning-configuration Status=Enabled
```

Exemple: Suspendre la gestion des versions S3

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/bucket/example-outposts-bucket --versioning-configuration Status=Suspended
```

Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts

Vous pouvez utiliser S3 Lifecycle pour optimiser la capacité de stockage d'Amazon S3 sur Outposts. Vous pouvez créer des règles de cycle de vie pour faire expirer les objets quand ils vieillissent ou sont remplacés par des versions plus récentes. Vous pouvez créer, activer, désactiver ou supprimer une règle de cycle de vie.

Pour plus d'informations sur le cycle de vie S3, consultez [Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts](#).

Note

La personne Compte AWS qui crée le bucket en est propriétaire et est la seule à pouvoir créer, activer, désactiver ou supprimer une règle de cycle de vie.

Pour créer et gérer la configuration du cycle de vie de votre compartiment S3 on Outposts, consultez les rubriques suivantes.

Rubriques

- [Création et gestion d'une règle de cycle de vie à l'aide du AWS Management Console](#)
- [Création et gestion d'une configuration du cycle de vie à l'aide du SDK AWS CLI and pour Java](#)

Création et gestion d'une règle de cycle de vie à l'aide du AWS Management Console

Vous pouvez utiliser S3 Lifecycle pour optimiser la capacité de stockage d'Amazon S3 sur Outposts. Vous pouvez créer des règles de cycle de vie pour faire expirer les objets quand ils vieillissent ou sont remplacés par des versions plus récentes. Vous pouvez créer, activer, désactiver ou supprimer une règle de cycle de vie.

Pour plus d'informations sur le cycle de vie S3, consultez [Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts](#).

Note

La personne Compte AWS qui crée le bucket en est propriétaire et est la seule à pouvoir créer, activer, désactiver ou supprimer une règle de cycle de vie.

Pour créer et gérer une règle de cycle de vie pour un S3 sur Outposts à l'aide du AWS Management Console, consultez les rubriques suivantes.

Rubriques


- [Création d'une stratégie de cycle de vie](#)
- [Activer une stratégie de cycle de vie](#)
- [Modifier une stratégie de cycle de vie](#)
- [Supprimer une stratégie de cycle de vie](#)

Création d'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 panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Sélectionnez le compartiment Outposts pour lequel vous voulez créer une règle de cycle de vie.
4. Choisissez l'onglet Management (Gestion), puis Create lifecycle rule (Créer une règle de cycle de vie).
5. Saisissez une valeur pour Lifecycle rule name (Nom de la règle de cycle de vie).
6. Sous Rule scope (Portée de la règle), choisissez l'une des options suivantes :
 - Pour limiter la portée à des filtres spécifiques, choisissez Limit the scope of this rule using one or more filters (Limiter la portée de cette règle en utilisant un ou plusieurs filtres). Ensuite, ajoutez un filtre de préfixe, des identifications ou une taille d'objet.
 - Pour appliquer la règle à tous les objets du compartiment, choisissez Apply to all objects in the bucket (Appliquer à tous les objets du compartiment).

7. Sous Lifecycle rule actions (Actions de règle de cycle de vie), choisissez l'une des options suivantes :
- **Expire current versions of objects (Faire expirer les versions actuelles des objets)** : pour les compartiments compatibles avec la gestion des versions, S3 sur Outposts ajoute un marqueur de suppression et conserve les objets en tant que versions anciennes. Pour les compartiments qui n'utilisent pas la gestion des versions S3, S3 on Outposts supprime définitivement les objets.
 - **Permanently delete noncurrent versions of objects (Supprimer définitivement les versions anciennes des objets)** : S3 sur Outposts supprime définitivement les versions anciennes des objets.
 - **Delete expired object delete markers or incomplete multipart uploads (Supprimer les marqueurs de suppression d'objet expirés ou les chargements partitionnés non terminés)** : S3 sur Outposts supprime définitivement les marqueurs de suppression d'objet expirés ou les chargements partitionnés non terminés.

Si vous limitez la portée de votre règle de cycle de vie en utilisant des balises d'objet, vous ne pouvez pas choisir **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)**. Vous ne pouvez pas non plus choisir **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)** si vous choisissez **Expire current object versions (Faire expirer les versions actuelles des objets)**.

 Note

Les filtres basés sur la taille ne peuvent pas être utilisés avec des marqueurs de suppression et des chargements partitionnés non terminés.

8. Si vous avez choisi **Expire current versions of objects (Faire expirer les versions actuelles des objets)** ou **Permanently delete noncurrent versions of objects (Supprimer définitivement les versions anciennes des objets)**, configurez le déclencheur de règles en fonction d'une date spécifique ou de l'âge de l'objet.
9. Si vous avez choisi **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)**, pour confirmer que vous souhaitez supprimer les marqueurs de suppression d'objets expirés, sélectionnez **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)**.

10. Sous Timeline Summary (Récapitulatif de la chronologie), vérifiez votre règle de cycle de vie et choisissez Create rule (Créer une règle).

Activer une stratégie de cycle de vie

Pour activer ou désactiver une règle de cycle de vie de compartiment


1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts pour lequel vous voulez activer ou désactiver une règle de cycle de vie.
4. Choisissez l'onglet Management (Gestion), puis sous Lifecycle rule (Règle de cycle de vie), choisissez la règle que vous voulez activer ou désactiver.
5. Pour Action, choisissez Enable or disable rule (Activer ou désactiver la règle).

Modifier une stratégie de cycle de vie

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts pour lequel vous voulez modifier une règle de cycle de vie.
4. Choisissez l'onglet Management (Gestion), puis la règle de cycle de vie que vous voulez modifier.
5. (Facultatif) Mettez à jour la valeur de Lifecycle rule name (Nom de la règle de cycle de vie).
6. Sous Rule scope (Portée de la règle), modifiez la portée selon vos besoins :
 - Pour limiter la portée à des filtres spécifiques, choisissez Limit the scope of this rule using one or more filters (Limiter la portée de cette règle en utilisant un ou plusieurs filtres). Ensuite, ajoutez un filtre de préfixe, des identifications ou une taille d'objet.
 - Pour appliquer la règle à tous les objets du compartiment, choisissez Apply to all objects in the bucket (Appliquer à tous les objets du compartiment).
7. Sous Lifecycle rule actions (Actions de règle de cycle de vie), choisissez l'une des options suivantes :

- **Expire current versions of objects (Faire expirer les versions actuelles des objets)** : pour les compartiments compatibles avec la gestion des versions, S3 sur Outposts ajoute un marqueur de suppression et conserve les objets en tant que versions anciennes. Pour les compartiments qui n'utilisent pas la gestion des versions S3, S3 on Outposts supprime définitivement les objets.
- **Permanently delete noncurrent versions of objects (Supprimer définitivement les versions anciennes des objets)** : S3 sur Outposts supprime définitivement les versions anciennes des objets.
- **Delete expired object delete markers or incomplete multipart uploads (Supprimer les marqueurs de suppression d'objet expirés ou les chargements partitionnés non terminés)** : S3 sur Outposts supprime définitivement les marqueurs de suppression d'objet expirés ou les chargements partitionnés non terminés.

Si vous limitez la portée de votre règle de cycle de vie en utilisant des balises d'objet, vous ne pouvez pas choisir **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)**. Vous ne pouvez pas non plus choisir **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)** si vous choisissez **Expire current object versions (Faire expirer les versions actuelles des objets)**.

 Note

Les filtres basés sur la taille ne peuvent pas être utilisés avec des marqueurs de suppression et des chargements partitionnés non terminés.

8. Si vous avez choisi **Expire current versions of objects (Faire expirer les versions actuelles des objets)** ou **Permanently delete noncurrent versions of objects (Supprimer définitivement les versions anciennes des objets)**, configurez le déclencheur de règles en fonction d'une date spécifique ou de l'âge de l'objet.
9. Si vous avez choisi **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)**, pour confirmer que vous souhaitez supprimer les marqueurs de suppression d'objets expirés, sélectionnez **Delete expired object delete markers (Supprimer les marqueurs de suppression d'objets expirés)**.
10. Choisissez **Enregistrer**.

Supprimer une stratégie de cycle de vie

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).
3. Choisissez le compartiment Outposts pour lequel vous voulez supprimer une règle de cycle de vie.
4. Choisissez l'onglet Management (Gestion), puis sous Lifecycle rule (Règle de cycle de vie), choisissez la règle que vous voulez supprimer.
5. Sélectionnez Supprimer.

Création et gestion d'une configuration du cycle de vie à l'aide du SDK AWS CLI and pour Java

Vous pouvez utiliser S3 Lifecycle pour optimiser la capacité de stockage d'Amazon S3 sur Outposts. Vous pouvez créer des règles de cycle de vie pour faire expirer les objets quand ils vieillissent ou sont remplacés par des versions plus récentes. Vous pouvez créer, activer, désactiver ou supprimer une règle de cycle de vie.

Pour plus d'informations sur le cycle de vie S3, consultez [Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts](#).

Note

La personne Compte AWS qui crée le bucket en est propriétaire et est la seule à pouvoir créer, activer, désactiver ou supprimer une règle de cycle de vie.

Pour créer et gérer une configuration de cycle de vie pour un bucket S3 on Outposts à l'aide de AWS Command Line Interface (AWS CLI) et du AWS SDK pour Java, consultez les exemples suivants.

Rubriques

- [Exécution d'une commande de configuration PUT](#)
- [Exécution d'une commande de configuration de cycle de vie GET pour un compartiment S3 on Outposts](#)

Exécution d'une commande de configuration PUT

AWS CLI

L' AWS CLI exemple suivant place une politique de configuration du cycle de vie dans un bucket Outposts. Cette stratégie spécifie que tous les objets dont le préfixe est labelisé (*myprefix*), ainsi que les balises, expirent après 10 jours. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

1. Enregistrez la stratégie de configuration du cycle de vie dans un fichier JSON. Dans cet exemple, le fichier est nommé `lifecycle1.json`.

```
{
  "Rules": [
    {
      "ID": "id-1",
      "Filter": {
        "And": {
          "Prefix": "myprefix",
          "Tags": [
            {
              "Value": "mytagvalue1",
              "Key": "mytagkey1"
            },
            {
              "Value": "mytagvalue2",
              "Key": "mytagkey2"
            }
          ],
          "ObjectSizeGreaterThan": 1000,
          "ObjectSizeLessThan": 5000
        }
      },
      "Status": "Enabled",
      "Expiration": {
        "Days": 10
      }
    }
  ]
}
```

- 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. Pour plus d'informations sur cette commande, reportez-vous [put-bucket-lifecycle-configuration](#) à la section AWS CLI Référence.

```
aws s3control put-bucket-lifecycle-configuration --account-id 123456789012 --
bucket arn:aws:s3-outposts:region:123456789012:outpost/op-01ac5d28a6a232904/
bucket/example-outposts-bucket --lifecycle-configuration file://lifecycle1.json
```

SDK for Java

L'exemple d'utilisation de SDK pour Java suivant place une configuration de cycle de vie sur un compartiment Outposts. Cette configuration de cycle de vie spécifie que tous les objets dont le préfixe est labelisé (*myprefix*), ainsi que les balises, expirent après 10 jours. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations. Pour plus d'informations, consultez [PutBucketLifecycleConfiguration](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void putBucketLifecycleConfiguration(String bucketArn) {

    S3Tag tag1 = new S3Tag().withKey("mytagkey1").withValue("mytagkey1");
    S3Tag tag2 = new S3Tag().withKey("mytagkey2").withValue("mytagkey2");

    LifecycleRuleFilter lifecycleRuleFilter = new LifecycleRuleFilter()
        .withAnd(new LifecycleRuleAndOperator()
            .withPrefix("myprefix")
            .withTags(tag1, tag2))
            .withObjectSizeGreaterThan(1000)
            .withObjectSizeLessThan(5000);

    LifecycleExpiration lifecycleExpiration = new LifecycleExpiration()
        .withExpiredObjectDeleteMarker(false)
        .withDays(10);

    LifecycleRule lifecycleRule = new LifecycleRule()
        .withStatus("Enabled")
        .withFilter(lifecycleRuleFilter)
        .withExpiration(lifecycleExpiration)
        .withID("id-1");
```

```
LifecycleConfiguration lifecycleConfiguration = new LifecycleConfiguration()
    .withRules(lifecycleRule);

PutBucketLifecycleConfigurationRequest reqPutBucketLifecycle = new
PutBucketLifecycleConfigurationRequest()
    .withAccountId(AccountId)
    .withBucket(bucketArn)
    .withLifecycleConfiguration(lifecycleConfiguration);

PutBucketLifecycleConfigurationResult respPutBucketLifecycle =
s3ControlClient.putBucketLifecycleConfiguration(reqPutBucketLifecycle);
System.out.printf("PutBucketLifecycleConfiguration Response: %s%n",
respPutBucketLifecycle.toString());
}
```

Exécution d'une commande de configuration de cycle de vie GET pour un compartiment S3 on Outposts

AWS CLI

L' AWS CLI exemple suivant permet d'obtenir une configuration du cycle de vie dans un bucket Outposts. Pour utiliser cette commande, remplacez chaque *user input placeholder* par vos propres informations. Pour plus d'informations sur cette commande, reportez-vous [get-bucket-lifecycle-configuration](#) à la section AWS CLI Référence.

```
aws s3control get-bucket-lifecycle-configuration --account-id 123456789012 --bucket
arn:aws:s3-outposts:<your-region>:123456789012:outpost/op-01ac5d28a6a232904/
bucket/example-outposts-bucket
```

SDK for Java

L'exemple d'utilisation de SDK pour Java suivant obtient une configuration de cycle de vie pour un compartiment Outposts. Pour plus d'informations, consultez [GetBucketLifecycleConfiguration](#) dans la Référence d'API Amazon Simple Storage Service.

```
import com.amazonaws.services.s3control.model.*;

public void getBucketLifecycleConfiguration(String bucketArn) {
```

```
GetBucketLifecycleConfigurationRequest reqGetBucketLifecycle = new
GetBucketLifecycleConfigurationRequest()
    .withAccountId(AccountId)
    .withBucket(bucketArn);

GetBucketLifecycleConfigurationResult respGetBucketLifecycle =
s3ControlClient.getBucketLifecycleConfiguration(reqGetBucketLifecycle);
System.out.printf("GetBucketLifecycleConfiguration Response: %s%n",
respGetBucketLifecycle.toString());
}
```

Répliquer des objets pour S3 sur Outposts

Lorsque la réplication S3 est activée AWS Outposts, vous pouvez configurer Amazon S3 on Outposts pour répliquer automatiquement les objets S3 sur différents Outposts ou entre des compartiments d'un même Outpost. Vous pouvez utiliser la réplication S3 sur Outposts pour gérer plusieurs réplicas de vos données dans le même Outpost ou dans des Outposts différents, ou sur différents comptes, afin de répondre aux besoins en matière de résidence des données. La réplication S3 sur Outposts permet de répondre à vos besoins de stockage conformes et de partager des données entre comptes. Si vous devez vous assurer que vos répliques sont identiques aux données sources, vous pouvez utiliser S3 Replication on Outposts pour créer des répliques de vos objets qui conservent toutes les métadonnées, telles que l'heure de création, les balises et la version de l'objet d'origine. IDs

La réplication S3 sur Outposts fournit également des métriques et des notifications détaillées pour surveiller le statut de la réplication des objets entre les compartiments. Vous pouvez utiliser Amazon CloudWatch pour surveiller la progression de la réplication en suivant les octets en attente de réplication, les opérations en attente de réplication et la latence de réplication entre vos compartiments source et de destination. Pour diagnostiquer et corriger rapidement les problèmes de configuration, vous pouvez également configurer Amazon EventBridge pour recevoir des notifications concernant les défaillances des objets de réplication. Pour en savoir plus, veuillez consulter la section [Gestion de votre réplication](#).

Rubriques

- [Configuration de réplication](#)
- [Exigences pour la réplication S3 sur Outposts](#)
- [Ce qui est répliqué](#)

- [Ce qui n'est pas répliqué](#)
- [Qu'est-ce qui n'est pas pris en charge par la réplication S3 sur Outposts ?](#)
- [Configuration de la réplication](#)
- [Gestion de votre réplication](#)

Configuration de réplication

S3 sur Outposts stocke une configuration de réplication au format XML. Dans le fichier XML de configuration de réplication, vous spécifiez un rôle Gestion des identités et des accès AWS (IAM) et une ou plusieurs règles.

```
<ReplicationConfiguration>
  <Role>IAM-role-ARN</Role>
  <Rule>
    ...
  </Rule>
  <Rule>
    ...
  </Rule>
  ...
</ReplicationConfiguration>
```

S3 sur Outposts ne peut pas répliquer d'objets sans votre autorisation. Vous accordez des autorisations S3 sur Outposts avec le rôle IAM que vous spécifiez dans la configuration de réplication. S3 sur Outposts endosse le rôle IAM pour répliquer des objets en votre nom. Vous devez accorder les autorisations requises au rôle IAM avant de commencer la réplication. Pour plus d'informations sur ces autorisations pour S3 sur Outposts, consultez [Création d'un rôle IAM](#).

Vous ajoutez une règle dans la configuration de réplication pour les scénarios suivants :

- Vous souhaitez répliquer tous les objets.
- Vous souhaitez répliquer un 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.

Vous ajoutez plusieurs règles dans une configuration de réplication si vous souhaitez répliquer un sous-ensemble d'objets distinct. Dans chaque règle, vous spécifiez un filtre qui sélectionne un sous-

ensemble d'objets 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 la configuration et les règles de réplication de S3 on Outposts, consultez [ReplicationConfiguration](#) le manuel Amazon Simple Storage Service API Reference.

Exigences pour la réplication S3 sur Outposts

La réplication exige de respecter les conditions suivantes :

- La plage d'adresses CIDR Outpost de destination doit être associée à votre table de sous-réseau Outpost source. Pour de plus amples informations, veuillez consulter [Conditions préalables à la création de règles de réplication](#).
- La gestion des versions S3 doit être activée pour les compartiments source et de destination. Pour plus d'informations sur la gestion des versions, consultez [Gestion de la gestion des versions S3 pour votre compartiment S3 sur Outposts](#).
- Amazon S3 sur Outposts doit disposer des autorisations adéquates pour répliquer en votre nom les objets issus du compartiment source vers le compartiment de destination. Cela signifie que vous devez créer une fonction du service pour déléguer des autorisations GET et PUT à S3 sur Outposts.
 1. Avant de créer la fonction du service, vous devez disposer d'une autorisation GET sur le compartiment source et d'une autorisation PUT sur le compartiment de destination.
 2. Pour créer la fonction du service permettant de déléguer des autorisations à S3 sur Outposts, vous devez d'abord configurer les autorisations afin de permettre à une entité IAM (utilisateur ou rôle) d'effectuer les actions `iam:CreateRole` et `iam:PassRole`. Enfin, vous autorisez l'entité IAM à créer une fonction du service. Afin de faire endosser à S3 sur Outposts la fonction du service en votre nom et déléguer des autorisations GET et PUT à S3 sur Outposts, vous devez attribuer les stratégies d'approbation et d'autorisation nécessaires au rôle. Pour plus d'informations sur ces autorisations pour S3 sur Outposts, consultez [Création d'un rôle IAM](#). Pour plus d'informations sur la création d'une fonction du service, consultez [Creating a service role](#) (Création d'une fonction du service).

Ce qui est répliqué

Par défaut, S3 sur Outposts réplique les éléments suivants :

- Objets créés après l'ajout d'une configuration de réplication.

- Métadonnées d'objet des objets source vers les réplicas. Pour plus d'informations sur la réplication des métadonnées des réplicas vers les objets source, consultez [Statut de la réplication si la synchronisation des modifications de réplica Amazon S3 sur Outposts est activée](#).
- Les balises d'objets, le cas échéant.

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 effectuez une demande DELETE sans spécifier d'ID de version d'objet, S3 sur Outposts ajoute un marqueur de suppression. S3 sur Outposts traite le marqueur de suppression comme suit :
 - S3 sur Outposts 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 plus d'informations sur la façon d'activer la réplication d'un marqueur de suppression dans votre configuration de réplication, consultez [Utilisation de la console S3](#).
- Si vous spécifiez un ID de version d'objet à supprimer dans une demande DELETE, S3 sur Outposts supprime de façon permanente cette version de l'objet dans le compartiment source. Cependant, 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. Ce comportement protège les données des suppressions malveillantes.

Ce qui n'est pas répliqué

Par défaut, S3 sur Outposts 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.
- 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, S3 sur Outposts ne procède pas à une nouvelle réplication des objets.

- Objets créés avec le chiffrement côté serveur à l'aide de clés de chiffrement fournies par le client (SSE-C).
- 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 dans votre compartiment source et que vous configurez des actions d'expiration, S3 sur Outposts crée des marqueurs de suppression pour les objets expirés dans le compartiment source, mais ne réplique pas ces marqueurs dans les compartiments de destination. 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 [Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts](#).

Qu'est-ce qui n'est pas pris en charge par la réplication S3 sur Outposts ?

Les fonctions de réplication S3 suivantes ne sont actuellement pas prises en charge par S3 sur Outposts :

- Contrôle du temps de réplication S3 (S3 RTC). S3 RTC n'est pas pris en charge car le trafic d'objets dans la réplication S3 sur Outposts passe par votre réseau sur site (la passerelle locale). Pour plus d'informations sur les passerelles locales, consultez [Working with the local gateway](#) (Utilisation des passerelles locales) dans le Guide de l'utilisateur AWS Outposts .
- Réplication S3 pour les opérations par lot.

Configuration de la réplication

Note

Les objets qui existaient dans votre compartiment avant la configuration de la règle de réplication ne sont pas répliqués automatiquement. En d'autres termes, Amazon S3 sur Outposts ne réplique pas les objets de manière rétroactive. Pour répliquer des objets créés

avant la configuration de votre réplication, vous pouvez utiliser l'opération d'API `CopyObject` pour les copier dans le même compartiment. Une fois les objets copiés, ils apparaissent en tant que « nouveaux » objets dans le compartiment et la configuration de réplication s'appliquera à eux. Pour plus d'informations sur la copie d'un objet, consultez [Copier un objet dans un compartiment Amazon S3 on Outposts à l'aide du AWS SDK pour Java](#) et [CopyObject](#) dans la Référence d'API Amazon Simple Storage Service.

Pour activer la réplication S3 sur Outposts, ajoutez une règle de réplication à votre compartiment Outposts source. La règle de réplication indique à S3 sur Outposts de répliquer les objets comme spécifié. Dans la règle de réplication, vous devez renseigner les éléments suivants :

- Point d'accès au compartiment Outposts source : Amazon Resource Name (ARN) du point d'accès ou alias du point d'accès du compartiment à partir duquel vous souhaitez que S3 sur Outposts réplique les objets S3. Pour plus d'informations sur l'utilisation des alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).
- Objets que vous voulez répliquer : vous pouvez répliquer l'ensemble ou un sous-ensemble des objets du compartiment Outposts source. 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/`, S3 sur Outposts réplique les objets avec des 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, S3 sur Outposts réplique uniquement les objets dotés du préfixe de clé et des balises spécifiques.

- Compartiment Outposts de destination : ARN ou alias de point d'accès du compartiment vers lequel vous souhaitez que S3 sur Outposts réplique les objets.

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

S3 sur Outposts fournit également des opérations d'API 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

- [Conditions préalables à la création de règles de réplication](#)
- [Création de règles de réplication sur Outposts](#)

Conditions préalables à la création de règles de réplication

Rubriques

- [Connexion de vos sous-réseaux Outpost source et de destination](#)
- [Création d'un rôle IAM](#)

Connexion de vos sous-réseaux Outpost source et de destination

Pour que votre trafic de réplication passe de votre Outpost source à votre Outpost de destination via votre passerelle locale, vous devez ajouter un nouvel acheminement pour configurer la mise en réseau. Vous devez connecter les plages de réseau de routage inter-domaines sans classe (CIDR) de vos points d'accès. Pour chaque paire de points d'accès, vous ne devez configurer cette connexion qu'une seule fois.

Certaines étapes de configuration de la connexion sont différentes, en fonction du type d'accès de vos points de terminaison Outposts associés à vos points d'accès. Le type d'accès pour les points de terminaison est soit privé (routage direct dans le cloud privé virtuel [VPC] AWS Outposts pour), soit IP appartenant au client (pool d'adresses IP [pool CoIP] appartenant au client au sein de votre réseau local).

Étape 1 : Trouver la plage CIDR de votre point de terminaison Outposts source

Pour trouver la plage CIDR de votre point de terminaison source associé à votre point d'accès 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 panneau de navigation de gauche, choisissez Outposts buckets (Compartiments Outposts).

3. Dans la liste Compartiments Outposts, choisissez le compartiment source à partir duquel vous souhaitez effectuer la réplique.
4. Choisissez l'onglet Points d'accès Outposts, puis choisissez le point d'accès Outposts pour le compartiment source de votre règle de réplique.
5. Sélectionnez le point de terminaison Outposts.
6. Copiez l'ID de sous-réseau à utiliser à [l'étape 5](#).
7. La méthode que vous utilisez pour trouver la plage d'adresses CIDR du point de terminaison Outposts source dépend du type d'accès de votre point de terminaison.

Dans la section Présentation du point de terminaison Outposts, consultez Type d'accès.

- Si le type d'accès est Privé, copiez la valeur CIDR (Classless Inter-Domain Routing) à utiliser à [l'étape 6](#).
- Si le type d'accès est Adresse IP détenue par le client, procédez comme suit :
 1. Copiez la valeur du IPv4 pool appartenant au client pour l'utiliser ultérieurement comme ID du pool d'adresses.
 2. Ouvrez la AWS Outposts console à l'adresse <https://console.aws.amazon.com/outposts/>.
 3. Dans le panneau de navigation, choisissez Tables de routage de passerelle locale.
 4. Choisissez la valeur ID de table de routage de passerelle locale de votre Outpost source.
 5. Dans le volet des détails, choisissez l'onglet Groupes CoIP. Collez la valeur de votre ID de groupe CoIP que vous avez copié précédemment dans le champ de recherche.
 6. Pour le pool CoIP correspondant, copiez la CIDR valeur correspondante de votre point de terminaison Outposts source pour l'utiliser [à l'étape 6](#).

Étape 2 : Trouver l'ID de sous-réseau et la plage d'adresses CIDR de votre point de terminaison Outposts de destination

Pour trouver l'ID de sous-réseau et la plage d'adresses CIDR de votre point de terminaison de destination associé à votre point d'accès de destination, suivez les mêmes sous-étapes à [l'étape 1](#) et remplacez votre point de terminaison Outposts source par votre point de terminaison Outposts de destination lorsque vous appliquez ces sous-étapes. Copiez la valeur de l'ID de sous-réseau de votre point de terminaison Outposts de destination pour l'utiliser à [l'étape 6](#). Copiez la valeur CIDR de votre point de terminaison Outposts de destination pour l'utiliser à [l'étape 5](#).

Étape 3 : Trouver l'ID de passerelle local de votre Outpost source

Pour trouver l'ID de passerelle local de votre Outpost source

1. Ouvrez la AWS Outposts console à l'adresse <https://console.aws.amazon.com/outposts/>.
2. Dans le volet de navigation de gauche, sélectionnez Passerelles locales.
3. Sur la page Passerelles locales, trouvez l'ID Outpost de votre Outpost source que vous souhaitez utiliser pour la réplication.
4. Copiez la valeur d'ID de passerelle locale de votre Outpost source pour l'utiliser à [l'étape 5](#).

Pour plus d'informations sur les passerelles locales, consultez [Local gateway](#) (Passerelles locales) dans le Guide de l'utilisateur AWS Outposts .

Étape 4 : Trouver l'ID de passerelle local de votre Outpost de destination

Pour trouver l'ID de passerelle locale de votre Outpost de destination, suivez les mêmes sous-étapes qu'à [l'étape 3](#), sauf que vous recherchez l'ID Outpost de votre Outpost de destination. Copiez la valeur d'ID de passerelle locale de votre Outpost de destination pour l'utiliser à [l'étape 6](#).

Étape 5 : Configurer la connexion entre votre sous-réseau Outpost source et votre sous-réseau Outpost de destination

Pour connecter votre sous-réseau Outpost source et votre sous-réseau Outpost de destination

1. Connectez-vous à la console VPC AWS Management Console et ouvrez-la à l'adresse. <https://console.aws.amazon.com/vpc/>
2. Dans le panneau de navigation de gauche, choisissez Subnets (Sous-réseaux).
3. Dans la zone de recherche, entrez l'ID de sous-réseau de votre point de terminaison Outposts source que vous avez trouvé à [l'étape 1](#). Choisissez le sous-réseau au sein de l'ID de sous-réseau correspondant.
4. Pour l'élément de sous-réseau correspondant, choisissez la valeur Table de routage de ce sous-réseau.
5. Sur la page contenant une table de routage sélectionnée, choisissez Actions, puis choisissez Modifier les routages.
6. Sur la page Modifier les routes, choisissez Ajouter une route.
7. Sous Destination, saisissez la plage d'adresses CIDR du point de terminaison Outposts de destination que vous avez trouvé à [l'étape 2](#).

8. Sous Cible, choisissez Passerelle locale de l'Outpost et saisissez l'ID de passerelle locale de votre Outpost source que vous avez trouvé à [l'étape 3](#).
9. Sélectionnez Enregistrer les modifications.
10. Assurez-vous que le Statut de la route est Actif.

Étape 6 : Configurer la connexion entre votre sous-réseau Outpost de destination et votre sous-réseau Outpost source

1. Connectez-vous à la console VPC AWS Management Console et ouvrez-la à l'adresse. <https://console.aws.amazon.com/vpc/>
2. Dans le panneau de navigation de gauche, choisissez Subnets (Sous-réseaux).
3. Dans la zone de recherche, saisissez l'ID de sous-réseau de votre point de terminaison Outposts de destination que vous avez trouvé à [l'étape 2](#). Choisissez le sous-réseau au sein de l'ID de sous-réseau correspondant.
4. Pour l'élément de sous-réseau correspondant, choisissez la valeur Table de routage de ce sous-réseau.
5. Sur la page contenant une table de routage sélectionnée, choisissez Actions, puis choisissez Modifier les routages.
6. Sur la page Modifier les routes, choisissez Ajouter une route.
7. Sous Destination, saisissez la plage d'adresses CIDR du point de terminaison Outposts source que vous avez trouvé à [l'étape 1](#).
8. Sous Cible, choisissez Passerelle locale de l'Outpost et saisissez l'ID de passerelle locale de votre Outpost de destination que vous avez trouvé à [l'étape 4](#).
9. Sélectionnez Enregistrer les modifications.
10. Assurez-vous que le Statut de la route est Actif.

Après avoir connecté les plages réseau CIDR de vos points d'accès source et de destination, vous devez créer un rôle Gestion des identités et des accès AWS (IAM).

Création d'un rôle IAM

Par défaut, toutes les ressources S3 sur Outposts (compartiments, objets et sous-ressources liées) sont privées : seul le propriétaire des ressources peut y accéder. S3 sur Outposts a besoin d'autorisations pour lire et répliquer les objets du compartiment Outposts source. Vous accordez ces

autorisations en créant une fonction du service IAM et en spécifiant ce rôle dans votre configuration de réplication.

Cette section décrit la stratégie d'approbation et la stratégie d'autorisation minimale requise. 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 [Création de règles de réplication sur Outposts](#). 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'approbation selon laquelle vous identifiez S3 sur Outposts en tant que principal de service capable d'endosser le rôle.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3-outposts.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- L'exemple suivant illustre une stratégie d'accès selon laquelle vous accordez au rôle les autorisations lui permettant d'effectuer les tâches de réplication en votre nom. Quand S3 sur Outposts endosse le rôle, il dispose des autorisations que vous avez spécifiées dans cette stratégie. Pour utiliser cette politique, remplacez *user input placeholders* par vos propres informations. Assurez-vous de les remplacer par l'Outpost IDs de vos Outposts source et de destination, ainsi que par les noms de bucket et de point d'accès de vos buckets Outposts source et de destination.

JSON

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

```

    "Action": [
      "s3-outposts:GetObjectVersionForReplication",
      "s3-outposts:GetObjectVersionTagging"
    ],
    "Resource": [
      "arn:aws:s3-outposts:us-east-1:123456789012:outpost/SOURCE-OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET/object/*",
      "arn:aws:s3-outposts:us-east-1:123456789012:outpost/SOURCE-OUTPOST-ID/accesspoint/SOURCE-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3-outposts:ReplicateObject",
      "s3-outposts:ReplicateDelete"
    ],
    "Resource": [
      "arn:aws:s3-outposts:us-east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET/object/*",
      "arn:aws:s3-outposts:us-east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
    ]
  }
]
}

```

La stratégie d'accès octroie les autorisations pour les actions suivantes :

- `s3-outposts:GetObjectVersionForReplication` : l'autorisation pour cette action est accordée sur tous les objets afin de permettre à S3 sur Outposts d'obtenir une version d'objet spécifique associée à chaque objet.
- `s3-outposts:GetObjectVersionTagging` : l'autorisation pour cette action sur des objets du compartiment `SOURCE-OUTPOSTS-BUCKET` (compartiment source) permet à S3 sur Outposts de lire les balises d'objets pour la réplication. Pour de plus amples informations, veuillez consulter [Ajout de balises pour les compartiments Amazon S3 on Outposts](#). Si S3 sur Outposts ne dispose pas de ces autorisations, il réplique les objets mais pas leurs balises.
- `s3-outposts:ReplicateObject` et `s3-outposts:ReplicateDelete` : les autorisations pour ces actions sur tous les objets du compartiment `DESTINATION-OUTPOSTS-BUCKET`

(compartiment cible) permettent à S3 sur Outposts de répliquer des objets ou des marqueurs de suppression dans le compartiment Outposts de destination. Pour en savoir plus sur les marqueurs de suppression, consultez [Impact des opérations de suppression sur la réplication](#).

Note

- L'autorisation pour l'action `s3-outposts:ReplicateObject` sur le compartiment *DESTINATION-OUTPOSTS-BUCKET* (compartiment de destination) permet également la réplication des balises d'objets. Il n'est donc pas nécessaire d'accorder une autorisation explicite pour l'action `s3-outposts:ReplicateTags`.
- Pour la réplication intercompte, le propriétaire du compartiment Outposts de destination doit mettre à jour sa politique de compartiment afin d'autoriser l'action `s3-outposts:ReplicateObject` sur *DESTINATION-OUTPOSTS-BUCKET*. L'action `s3-outposts:ReplicateObject` permet à S3 sur Outposts de répliquer des objets et des balises d'objet vers le compartiment Outposts de destination.

Pour obtenir la liste des actions S3 sur Outposts, consultez [Actions définies par Amazon S3 sur Outposts](#).

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 Outposts 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 de la politique de compartiment et de la politique de point d'accès. Dans le cas contraire, S3 sur Outposts ne peut pas accéder aux objets et la réplication des objets échoue.

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 S3 sur Outposts.

Octroi d'autorisations lorsque les buckets Outposts source et de destination appartiennent à différents Comptes AWS

Lorsque les compartiments Outposts source et de destination n'appartiennent pas aux mêmes comptes, le propriétaire du compartiment Outposts de destination doit mettre à jour les politiques de compartiment et de point d'accès du compartiment de destination. Ces politiques doivent accorder au propriétaire du compartiment Outposts source et à la fonction du service IAM les autorisations nécessaires pour effectuer des actions de réplication, comme indiqué dans les exemples de politiques suivants, faute de quoi la réplication échouera. Dans ces exemples de politique, *DESTINATION-OUTPOSTS-BUCKET* est le compartiment de destination. Pour utiliser ces exemples de politique, remplacez *user input placeholders* par vos propres informations.


Si vous créez la fonction du service IAM manuellement, définissez le chemin du rôle sur `role/service-role/`, comme indiqué dans les exemples de politique suivants. Pour plus d'informations, consultez la section [IAM ARNs](#) dans le guide de l'utilisateur d'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-outposts:ReplicateDelete",
        "s3-outposts:ReplicateObject"
      ],
      "Resource": [
        "arn:aws:s3-outposts:us-east-1:444455556666:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET/object/*"
      ]
    }
  ]
}
```

JSON

```
{
  "Version": "2012-10-17",
  "Id": "PolicyForDestinationAccessPoint",
  "Statement": [
    {
      "Sid": "Permissions on objects",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/service-role/source-account-IAM-role"
      },
      "Action": [
        "s3-outposts:ReplicateDelete",
        "s3-outposts:ReplicateObject"
      ],
      "Resource": [
        "arn:aws:s3-outposts:us-east-1:111122223333:outpost/DESTINATION-OUTPOST-ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
      ]
    }
  ]
}
```

 Note

Si des objets stockés dans le compartiment Outposts source sont balisés, notez les points suivants :

Si le propriétaire du compartiment Outposts source octroie à S3 sur Outposts l'autorisation d'effectuer les actions `s3-outposts:GetObjectVersionTagging` et `s3-outposts: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](#).

Création de règles de réplication sur Outposts

La réplication S3 sur Outposts est la réplication automatique et asynchrone d'objets entre des compartiments identiques ou différents. AWS Outposts Elle réplique les objets nouvellement créés et les mises à jour d'objets d'un compartiment Outposts source vers un ou plusieurs compartiments Outposts de destination. Pour de plus amples informations, veuillez consulter [Répliquer des objets pour S3 sur Outposts](#).

Note

Les objets qui existaient dans votre compartiment Outposts source avant la configuration des règles de réplication ne sont pas répliqués. En d'autres termes, S3 sur Outposts ne réplique pas les objets de manière rétroactive. Pour répliquer des objets créés avant la configuration de votre réplication, vous pouvez utiliser l'opération d'API `CopyObject` pour les copier dans le même compartiment. Une fois les objets copiés, ils apparaissent en tant que « nouveaux » objets dans le compartiment et la configuration de réplication s'appliquera à eux. Pour plus d'informations sur la copie d'un objet, consultez [Copier un objet dans un compartiment Amazon S3 on Outposts à l'aide du AWS SDK pour Java](#) et [CopyObject](#) dans la Référence d'API Amazon Simple Storage Service.

Lorsque vous configurez la réplication, vous ajoutez des règles de réplication au compartiment Outposts source. Les règles de réplication définissent les objets du compartiment Outposts source à répliquer, ainsi que le ou les compartiments Outposts 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 Outposts de destination peut se trouver dans le même Outpost que le compartiment Outposts source, mais il peut également se trouver dans un autre Outpost.

Pour les règles de réplication S3 sur Outposts, vous devez fournir à la fois l'Amazon Resource Name (ARN) du compartiment Outposts source et l'ARN du point d'accès du compartiment Outposts de destination au lieu des noms des compartiments Outposts source et de destination.

Si vous spécifiez un ID de version d'objet à supprimer, S3 sur Outposts supprime cette version de l'objet dans le compartiment Outposts source. Mais il ne réplique pas la suppression dans le compartiment Outposts de destination. En d'autres termes, il ne supprime pas la même version de l'objet dans le compartiment Outposts de destination. Ce comportement protège les données des suppressions malveillantes.

Lorsque vous ajoutez une règle de réplication à un compartiment Outposts, celle-ci est activée par défaut et entre en fonctionnement dès que vous l'enregistrez.

Dans cet exemple, vous configurez la réplication pour les compartiments Outposts source et de destination qui sont sur différents Outposts et 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. Pour plus d'informations sur les autorisations de réplication S3 intercompte sur Outposts, consultez [Octroi d'autorisations lorsque les buckets Outposts source et de destination appartiennent à différents Comptes AWS](#).

Pour connaître les conditions préalables aux règles de réplication S3 sur Outposts, consultez [Conditions préalables à la création de règles de réplication](#).

Utilisation de la console S3

Suivez ces étapes pour configurer une règle de réplication quand le compartiment Amazon S3 sur Outposts de destination se trouve dans un Outpost différent de celui du compartiment Outposts source.

Si le compartiment Outposts de destination se trouve dans un compte différent du compartiment Outposts source, vous devez ajouter une stratégie de compartiment au compartiment Outposts de destination pour accorder au propriétaire du compte du compartiment Outposts source l'autorisation d'effectuer des réplications d'objets dans le compartiment Outposts de destination.

Pour créer une règle 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 la liste Compartiments Outposts, choisissez le nom du compartiment que vous voulez utiliser comme compartiment source.
3. Sélectionnez Gestion, faites défiler jusqu'à la section Règles de réplication, puis sélectionnez Créer une règle de réplication.
4. 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.
5. 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.
6. Sous Priorité, la valeur de priorité de la règle détermine la règle à appliquer en cas de chevauchement de règles. Lorsque des objets sont inclus dans la portée de plusieurs règles de

réplication, S3 sur Outposts utilise ces valeurs de priorité pour éviter les conflits. Par défaut, les nouvelles règles sont ajoutées à la configuration de la réplication avec la priorité la plus élevée. Plus le nombre est élevé, plus la priorité est haute.


Pour modifier la priorité de la règle, après l'avoir enregistrée, choisissez le nom de la règle dans la liste des règles de réplication, choisissez Actions, puis Modifier la priorité.

7. Sous Compartiment source, vous disposez des options suivantes pour définir la source de réplication :
 - Pour répliquer l'ensemble du compartiment, choisissez Appliquer à tous les objets du compartiment.
 - Pour appliquer un filtrage par préfixe ou par balise à la source de réplication, choisissez Limiter la portée de cette règle en utilisant un ou plusieurs filtres. Vous pouvez combiner un préfixe et des balises.
 - Pour répliquer tous les objets ayant le même préfixe, sous Préfixe, entrez un préfixe dans la zone. Le filtre Préfixe permet de limiter la réplication à tous les objets dont le nom commence par la même chaîne (par exemple `pictures`).

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 balises d'objet identiques, sélectionnez Ajouter une balise 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 [Ajout de balises pour les compartiments Amazon S3 on Outposts](#).
8. Pour accéder à votre compartiment source S3 sur Outposts à des fins de réplication, sous Nom du point d'accès source, choisissez un point d'accès attaché au compartiment source.
9. Sous Destination, choisissez l'ARN du point d'accès du compartiment Outposts de destination dans lequel vous souhaitez que S3 sur Outposts réplique des objets. Le bucket Outposts de destination peut être identique ou différent Compte AWS du bucket Outposts source.

Si le compartiment de destination se trouve dans un compte différent du compartiment Outposts source, vous devez ajouter une stratégie de compartiment au compartiment Outposts de destination pour accorder au propriétaire du compte du compartiment Outposts source l'autorisation d'effectuer des réplifications d'objets dans le compartiment Outposts de destination. Pour de plus amples informations, veuillez consulter [Octroi d'autorisations lorsque les buckets Outposts source et de destination appartiennent à différents Comptes AWS](#).

 Note

Si la gestion des versions n'est pas activée sur le compartiment Outposts 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 de service Gestion des identités et des accès AWS (IAM) que S3 on Outposts peut assumer pour répliquer des objets en votre nom.

Pour configurer un rôle IAM, sous Rôle IAM, effectuez l'une des opérations suivantes :

- Pour que S3 sur Outposts crée un nouveau rôle IAM pour votre configuration de réplication, choisissez Choisir parmi les rôles IAM existants, puis Créer un nouveau rôle. Lorsque vous enregistrez la règle, une nouvelle stratégie est générée pour le rôle IAM correspondant aux compartiments Outposts source et cible que vous choisissez. Nous vous recommandons de choisir Créer un nouveau rôle.
- Vous pouvez également choisir d'utiliser un rôle IAM existant. Dans ce cas, vous devez choisir un rôle qui octroie à S3 sur Outposts les autorisations nécessaires pour la réplication. La réplication échoue si ce rôle n'accorde pas à S3 sur Outposts des autorisations suffisantes pour suivre votre règle de réplication.

Pour choisir un rôle existant, choisissez Choisir parmi les rôles IAM existants, puis choisissez le rôle dans le menu déroulant. Vous pouvez également choisir Saisir un ARN de rôle IAM, puis saisir l'Amazon Resource Name (ARN) du rôle.

 Important

Lorsque vous ajoutez une règle de réplication à un compartiment S3 sur Outposts, vous devez disposer des autorisations `iam:CreateRole` et `iam:PassRole` pour pouvoir créer et transmettre le rôle IAM qui accorde les autorisations de réplication S3 sur Outposts. 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. Tous les objets contenus dans des compartiments Outposts sont chiffrés par défaut. Pour plus d'informations sur le chiffrement S3 sur Outposts, consultez la section [Chiffrement des données dans S3 sur Outposts](#). Seuls les objets chiffrés à l'aide du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) peuvent être répliqués. La réplication d'objets chiffrés à l'aide

du chiffrement côté serveur avec des clés AWS Key Management Service (AWS KMS) (SSE-KMS) ou du chiffrement côté serveur avec des clés fournies par le client (SSE-C) n'est pas prise en charge.

12. Au besoin, vous disposez des options supplémentaires suivantes lors de la définition de la configuration de la règle de réplication :

- Si vous souhaitez activer les métriques de réplication S3 sur Outposts dans votre configuration de réplication, sélectionnez Métriques de réplication. Pour de plus amples informations, veuillez consulter [Surveillance de la progression avec des métriques de réplication](#).
- 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 [Impact des opérations de suppression sur la réplication](#).
- Si vous souhaitez répliquer les modifications de métadonnées apportées aux réplicas vers les objets sources, sélectionnez Synchronisation des modifications de réplique. Pour de plus amples informations, veuillez consulter [Statut de la réplication si la synchronisation des modifications de réplica Amazon S3 sur Outposts est activée](#).

13. Choisissez Créer une règle pour terminer.

Une fois que vous avez enregistré votre règle, vous pouvez la modifier, l'activer, la désactiver ou la supprimer. Pour ce faire, accédez à l'onglet Gestion du compartiment Outposts source, faites défiler la page jusqu'à la section Règles de réplication, choisissez votre règle, puis choisissez Modifier la règle.

À l'aide du AWS CLI

AWS CLI Pour configurer la réplication lorsque les compartiments Outposts source et de destination appartiennent à la même entité Compte AWS, procédez comme suit :

- Créez des compartiments Outposts source et de destination.
- Activez la gestion des versions sur les deux compartiments.
- Créez un rôle IAM qui octroie à S3 sur Outposts l'autorisation de répliquer des objets.
- Ajoutez la configuration de réplication au compartiment Outposts source.

Testez votre configuration pour la vérifier.

Pour configurer la réplication lorsque les compartiments Outposts source et de destination appartiennent à la même entité Compte AWS

1. Définissez un profil d'informations d'identification pour l' AWS CLI. Dans cet exemple, nous utilisons le nom de profil `acctA`. Pour plus d'informations sur la définition des profils d'informations d'identification, consultez [Named profiles](#) (Profils nommés) dans le Guide de l'utilisateur AWS Command Line Interface .

Important

Le profil que vous utilisez dans cet exercice doit disposer des autorisations nécessaires. Par exemple, dans la configuration de la réplication, vous spécifiez la fonction du service IAM que S3 sur Outposts peut endosser. Vous ne pouvez effectuer cette tâche que si le profil que vous utilisez dispose des autorisations `iam:CreateRole` et `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, le profil nommé disposera des autorisations adéquates pour exécuter toutes les tâches.

2. Créez un compartiment *source* et activez le contrôle de version sur ce dernier. La commande `create-bucket` suivante crée un compartiment `SOURCE-OUTPOSTS-BUCKET` dans la région USA Est (Virginie du Nord) (`us-east-1`). Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control create-bucket --bucket SOURCE-OUTPOSTS-BUCKET --outpost-id SOURCE-OUTPOST-ID --profile acctA --region us-east-1
```

La commande `put-bucket-versioning` suivante active la gestion des versions sur le compartiment `SOURCE-OUTPOSTS-BUCKET`. Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/bucket/SOURCE-OUTPOSTS-BUCKET --versioning-configuration Status=Enabled --profile acctA
```

3. Créez un compartiment de *destination* et activez le contrôle de version sur ce dernier. La commande `create-bucket` suivante crée un compartiment `DESTINATION-OUTPOSTS-`

BUCKET dans la région USA Ouest (Oregon) (us-west-2). Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

Note

Pour configurer une configuration de réplication lorsque les compartiments Outposts source et de destination se trouvent dans le même emplacement Compte AWS, vous devez utiliser le même profil. Cet exemple utilise *acctA*. Pour tester la configuration de réplication lorsque les buckets appartiennent à des propriétaires différents Comptes AWS, vous devez spécifier des profils différents pour chaque compartiment.

```
aws s3control create-bucket --bucket DESTINATION-OUTPOSTS-BUCKET --create-bucket-configuration LocationConstraint=us-west-2 --outpost-id DESTINATION-OUTPOST-ID --profile acctA --region us-west-2
```

La commande `put-bucket-versioning` suivante active la gestion des versions sur le compartiment *DESTINATION-OUTPOSTS-BUCKET*. Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

```
aws s3control put-bucket-versioning --account-id 123456789012 --bucket arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-OUTPOST-ID/bucket/DESTINATION-OUTPOSTS-BUCKET --versioning-configuration Status=Enabled --profile acctA
```

4. Créez une fonction du service IAM. Vous ajouterez cette fonction du service au compartiment *SOURCE-OUTPOSTS-BUCKET* plus tard dans la configuration de la réplication. S3 sur Outposts endosse ce rôle pour répliquer des objets en votre nom. Vous créez un rôle IAM en deux étapes.

- a. Créez un rôle IAM.

- i. Copiez la stratégie d'approbation suivante et enregistrez-la dans un fichier nommé `s3-on-outposts-role-trust-policy.json` dans le répertoire actif sur votre ordinateur local. Cette stratégie accorde au principal de service S3 sur Outposts les autorisations pour endosser cette fonction du service.

JSON

```
{
```

```

"Version":"2012-10-17",
"Statement":[
  {
    "Effect":"Allow",
    "Principal":{"
      "Service":"s3-outposts.amazonaws.com"
    },
    "Action":"sts:AssumeRole"
  }
]
}

```

- ii. Exécutez la commande suivante pour créer le rôle. Remplacez les *user input placeholders* par vos propres informations.

```

aws iam create-role --role-name replicationRole --assume-role-policy-
document file://s3-on-outposts-role-trust-policy.json --profile acctA

```

- b. Attachez une stratégie d'autorisation à la fonction du service.

- i. Copiez la politique d'autorisations suivante et enregistrez-la dans un fichier nommé `s3-on-outposts-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 S3 sur Outposts. Pour utiliser cette politique, remplacez *user input placeholders* par vos propres informations.

JSON

```

{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3-outposts:GetObjectVersionForReplication",
        "s3-outposts:GetObjectVersionTagging"
      ],
      "Resource": [
        "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/SOURCE-OUTPOST-ID/bucket/SOURCE-OUTPOSTS-
BUCKET/object/*",

```

```

        "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/SOURCE-OUTPOST-ID/accesspoint/SOURCE-
OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
    ],
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3-outposts:ReplicateObject",
            "s3-outposts:ReplicateDelete"
        ],
        "Resource": [
            "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/
bucket/DESTINATION-OUTPOSTS-BUCKET/object/*",
            "arn:aws:s3-outposts:us-
east-1:123456789012:outpost/DESTINATION-OUTPOST-ID/
accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT/object/*"
        ]
    }
]
}

```

- ii. Exécutez la commande suivante pour créer une stratégie et l'attacher au rôle. Remplacez les *user input placeholders* par vos propres informations.

```

aws iam put-role-policy --role-name replicationRole --policy-
document file://s3-on-outposts-role-permissions-policy.json --policy-
name replicationRolePolicy --profile acctA

```

5. Ajoutez une configuration de réplication au compartiment *SOURCE-OUTPOSTS-BUCKET*.
 - a. Bien que l'API S3 on Outposts nécessite une configuration de réplication au format XML, vous devez spécifier la AWS CLI configuration de réplication au format JSON. Enregistrez la configuration JSON dans un fichier (*replication.json*) dans le répertoire local de votre ordinateur. Pour utiliser cette configuration, remplacez *user input placeholders* par vos propres informations.

```

{
  "Role": "IAM-role-ARN",
  "Rules": [
    {

```

```

    "Status": "Enabled",
    "Priority": 1,
    "DeleteMarkerReplication": { "Status": "Disabled" },
    "Filter" : { "Prefix": "Tax"},
    "Destination": {
      "Bucket":
        "arn:aws:s3-outposts:region:123456789012:outpost/DESTINATION-OUTPOST-
        ID/accesspoint/DESTINATION-OUTPOSTS-BUCKET-ACCESS-POINT"
    }
  }
]
}

```

- b. Pour ajouter la configuration de réplication à votre compartiment Outposts source, exécutez la commande `put-bucket-replication` suivante. Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

```

aws s3control put-bucket-replication --account-id 123456789012 --
bucket arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-
ID/bucket/SOURCE-OUTPOSTS-BUCKET --replication-configuration file://
replication.json --profile acctA

```

- c. Pour récupérer la configuration de réplication, utilisez la commande `get-bucket-replication`. Pour utiliser cette commande, remplacez *user input placeholders* par vos propres informations.

```

aws s3control get-bucket-replication --account-id 123456789012 --bucket
arn:aws:s3-outposts:region:123456789012:outpost/SOURCE-OUTPOST-ID/
bucket/SOURCE-OUTPOSTS-BUCKET --profile acctA

```

6. Testez la configuration dans la console Amazon S3 :

- Connectez-vous à la console Amazon S3 AWS Management Console et ouvrez-la à l'adresse <https://console.aws.amazon.com/s3/>.
- Dans le compartiment *SOURCE-OUTPOSTS-BUCKET*, créez un dossier nommé Tax.
- Ajoutez les exemples d'objets au dossier Tax du compartiment *SOURCE-OUTPOSTS-BUCKET*.
- Dans le compartiment *DESTINATION-OUTPOSTS-BUCKET*, vérifiez les éléments suivants :
 - S3 sur Outposts a répliqué les objets.

Note

Le temps nécessaire à S3 sur Outposts pour répliquer un objet dépend de la taille de ce dernier. Pour obtenir des informations sur la consultation du statut de la réplification, consultez [Obtention d'informations sur le statut de la réplification](#).

- Dans l'onglet Propriétés, le Statut de réplification est défini sur Réplica (afin d'indiquer qu'il s'agit d'un objet répliqué).

Gestion de votre réplification

Cette section décrit des options de configuration de réplification supplémentaires disponibles dans S3 sur Outposts, comment déterminer le statut de la réplification et comment résoudre des problèmes de réplification. Pour obtenir des informations sur la configuration de réplification de base, veuillez consulter [Configuration de la réplification](#).

Rubriques

- [Surveillance de la progression avec des métriques de réplification](#)
- [Obtention d'informations sur le statut de la réplification](#)
- [Résolution des problèmes de réplification](#)
- [Utilisation EventBridge pour la réplification S3 sur les Outposts](#)

Surveillance de la progression avec des métriques de réplification

La réplification S3 sur Outposts fournit des métriques détaillées pour les règles de réplification dans votre configuration de réplification. Avec les métriques de réplification, vous pouvez surveiller la progression de la réplification par intervalles de 5 minutes en suivant les octets en attente, la latence de réplification et les opérations en attente. Pour aider à résoudre les problèmes de configuration, vous pouvez également configurer Amazon EventBridge pour recevoir des notifications en cas d'échec de réplification.

Lorsque les métriques de réplification sont activées, S3 Replication on Outposts publie les métriques suivantes sur Amazon : CloudWatch

- Octets en attente de réplification : nombre total d'octets d'objets en attente de réplification pour une règle de réplification donnée.

- Latence de réplication : nombre maximal de secondes pendant lesquelles le compartiment de destination de réplication se trouve derrière le compartiment source pour une règle de réplication donnée.
- Opérations en attente de réplication : nombre d'opérations en attente de réplication pour une règle de réplication donnée. Les opérations incluent des objets, des marqueurs de suppression et des balises.

Note

Les métriques S3 Replication on Outposts sont facturées au même tarif que CloudWatch les métriques personnalisées. Pour en savoir plus, consultez [PricingCloudWatch](#) (Tarification).

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 par Amazon S3 sur Outposts. Le statut de réplication d'un objet source renvoie soit PENDING, COMPLETED ou FAILED. Le statut de réplication d'un réplica renvoie REPLICATED.

Vue d'ensemble des statuts de réplication

Dans un scénario de réplication, il existe un compartiment source dans lequel vous configurez la réplication et un compartiment de destination dans lequel S3 sur Outposts réplique les objets. Lorsque vous demandez un objet (avec `GetObject`) ou des métadonnées d'objet (avec `HeadObject`) à partir de ces compartiments, S3 sur Outposts renvoie l'en-tête `x-amz-replication-status` dans la réponse, comme suit :

- Lorsque vous demandez un objet depuis le compartiment source, S3 sur Outposts 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 S3 sur Outposts 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, S3 sur Outposts 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 recharger l'objet. Les objets passent à l'état FAILED en cas de problèmes, par exemple si les autorisations de rôle de réplication ou les autorisations de compartiment sont manquantes. Pour les échecs temporaires, par exemple si un compartiment ou votre Outpost n'est pas disponible, le statut de réplication ne passera pas à FAILED, mais restera PENDING. Une fois la ressource remise en ligne, S3 sur Outposts reprendra 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 S3 sur Outposts, S3 sur Outposts 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 vérifier qu'il a été répliqué.

Statut de la réplication si la synchronisation des modifications de réplica Amazon S3 sur Outposts est activée

Lorsque vos règles de réplication activent la synchronisation des modifications de réplica S3 sur Outposts, 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` du réplica renvoie `PENDING`. Si la synchronisation des modifications du réplica ne parvient pas à répliquer les métadonnées, l'en-tête du réplica renvoie `FAILED`. Si les métadonnées sont répliquées correctement, l'en-tête du réplica renvoie la valeur `REPLICA`.

Résolution des problèmes de réplication

Si les réplicas d'objets ne figurent pas dans le compartiment Amazon S3 sur Outposts de destination après la configuration de la réplication, utilisez les conseils de dépannage suivants pour identifier les problèmes et les résoudre.

- Le temps nécessaire à S3 sur Outposts pour répliquer un objet dépend de plusieurs facteurs, y compris de la distance entre la paire de régions source et de destination et de la taille de l'objet.

Vous pouvez vérifier le statut de réplication de l'objet source. Si le statut de réplication de l'objet est PENDING, cela signifie que S3 sur Outposts 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.

- Dans la configuration de réplication du compartiment source, procédez aux vérifications suivantes :
 - L'Amazon Resource Name (ARN) du point d'accès 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 est Enabled.
- Vérifiez que la gestion des versions n'a pas été suspendue sur aucun compartiment. La gestion des versions doit être activée pour les compartiments source et de destination.
- 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 [Octroi d'autorisations lorsque les buckets Outposts source et de destination appartiennent à différents Comptes AWS](#).
- Si un réplica d'objet ne figure pas dans le compartiment de destination, les problèmes suivants ont pu empêcher la réplication :
 - S3 sur Outposts 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, S3 sur Outposts ne réplique pas les réplicas d'objets dans le compartiment B vers le compartiment C.

Si vous souhaitez répliquer des objets du compartiment A vers le compartiment B et le compartiment C, définissez plusieurs destinations de compartiment selon différentes règles de réplication pour la configuration de la réplication de votre compartiment source. Par exemple, créez deux règles de réplication sur le compartiment source A, l'une pour la réplication vers le compartiment de destination B et l'autre pour la réplication vers le compartiment de destination 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 les problèmes de réplication, 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.
- 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 que S3 sur Outposts puisse répliquer l'objet. Si vous commencez par créer un objet, puis ajoutez la balise à l'objet existant, S3 sur Outposts ne réplique pas l'objet.
- La réplication échoue si la politique de compartiment refuse l'accès au rôle de réplication pour l'une des actions suivantes :

Compartiment source :

```
"s3-outposts:GetObjectVersionForReplication",  
"s3-outposts:GetObjectVersionTagging"
```

Compartiments de destination :

```
"s3-outposts:ReplicateObject",  
"s3-outposts:ReplicateDelete",  
"s3-outposts:ReplicateTags"
```

- Amazon EventBridge peut vous avertir lorsque les objets ne se répliquent pas vers leurs Outposts de destination. Pour de plus amples informations, veuillez consulter [Utilisation EventBridge pour la réplication S3 sur les Outposts](#).

Utilisation EventBridge pour la réplication S3 sur les Outposts

Amazon S3 on Outposts est intégré à Amazon EventBridge et utilise l'`s3-outposts` espace de noms. EventBridge est un service de bus d'événements sans serveur que vous pouvez utiliser pour connecter vos applications à des données provenant de diverses sources. Pour plus d'informations, consultez [Qu'est-ce qu'Amazon EventBridge ?](#) dans le guide de EventBridge l'utilisateur Amazon.

Pour aider à résoudre les problèmes de configuration de réplication, vous pouvez configurer Amazon EventBridge pour qu'il reçoive des notifications en cas d'échec de réplication. EventBridge peut vous avertir lorsque les objets ne se répliquent pas vers leurs Outposts de destination. Pour plus d'informations sur l'état actuel d'un objet répliqué, consultez [Vue d'ensemble des statuts de réplication](#).

Chaque fois que certains événements se produisent dans votre compartiment Outposts, S3 on Outposts peut envoyer des événements à EventBridge. Contrairement à d'autres destinations, vous n'avez pas besoin de sélectionner les types d'événements que vous souhaitez proposer. Vous pouvez également utiliser des EventBridge règles pour acheminer les événements vers des cibles supplémentaires. Une fois EventBridge activé, S3 on Outposts envoie tous les événements suivants à EventBridge.

Type d'événement	Description	Namespace
OperationFailedReplication	La réplication d'un objet au sein d'une règle de réplication a échoué. Pour plus d'informations sur les raisons de l'échec de la réplication S3 sur Outposts, consultez Utilisation EventBridge pour visualiser les raisons de l'échec de la réplication S3 sur les Outposts .	s3-outposts

Utilisation EventBridge pour visualiser les raisons de l'échec de la réplication S3 sur les Outposts

Le tableau suivant répertorie les raisons de l'échecs de la réplication S3 sur Outposts. Vous pouvez configurer une EventBridge règle pour publier et afficher la raison de l'échec via Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon AWS Lambda SNS) ou Amazon Logs. CloudWatch. Pour plus d'informations sur les autorisations requises pour utiliser ces ressources EventBridge, consultez la section [Utilisation de politiques basées sur les ressources](#) pour EventBridge.

Raison de l'échec de la réplication	Description
AssumeRoleNotPermitted	S3 on Outposts ne peut pas assumer le rôle Gestion des identités et des accès

Raison de l'échec de la réplication	Description
	AWS (IAM) spécifié dans la configuration de réplication.
DstBucketNotFound	S3 sur Outposts n'est pas en mesure de trouver le compartiment de destination spécifié dans la configuration de la réplication.
DstBucketUnversioned	La gestion des versions n'est pas activée sur le compartiment de destination Outposts. Pour répliquer des objets avec la réplication S3 sur Outposts, vous devez activer la gestion des versions pour le compartiment de destination.
DstDelObjNotPermitted	S3 sur Outposts n'est pas en mesure de répliquer les suppressions vers le compartiment de destination. L'autorisation <code>s3-outposts:ReplicateDelete</code> peut être manquante pour le compartiment de destination.
DstMultipartCompleteNotPermitted	S3 sur Outposts n'est pas en mesure de terminer le chargement partitionné des objets dans le compartiment de destination. L'autorisation <code>s3-outposts:ReplicateObject</code> peut être manquante pour le compartiment de destination.
DstMultipartInitNotPermitted	S3 sur Outposts n'est pas en mesure de lancer le chargement partitionné des objets vers le compartiment de destination. L'autorisation <code>s3-outposts:ReplicateObject</code> peut être manquante pour le compartiment de destination.

Raison de l'échec de la réplication	Description
<code>DstMultipartPartUploadNotPermitted</code>	S3 sur Outposts n'est pas en mesure de charger des objets de chargement partitionné dans le compartiment de destination. L'autorisation <code>s3-outposts:ReplicateObject</code> peut être manquante pour le compartiment de destination.
<code>DstOutOfCapacity</code>	S3 sur Outposts n'est pas en mesure de répliquer l'Outpost de destination car l'Outpost n'est pas compris dans la capacité de stockage de S3.
<code>DstPutObjNotPermitted</code>	S3 sur Outposts n'est pas en mesure de répliquer les objets vers le compartiment de destination. L'autorisation <code>s3-outposts:ReplicateObject</code> peut être manquante pour le compartiment de destination.
<code>DstPutTaggingNotPermitted</code>	S3 sur Outposts n'est pas en mesure de répliquer les balises d'objets vers le compartiment de destination. L'autorisation <code>s3-outposts:ReplicateObject</code> peut être manquante pour le compartiment de destination.
<code>DstVersionNotFound</code>	S3 sur Outposts n'est pas en mesure de trouver la version d'objet requise dans le compartiment de destination pour répliquer les métadonnées de cette version d'objet.
<code>SrcBucketReplicationConfigMissing</code>	S3 sur Outposts n'est pas en mesure de trouver une configuration de réplication pour le point d'accès associé au compartiment Outposts source.

Raison de l'échec de la réplication	Description
<code>SrcGetObjectNotPermitted</code>	S3 sur Outposts n'est pas en mesure d'accéder à l'objet dans le compartiment source pour la réplication. L'autorisation <code>s3-outposts:GetObjectVersionForReplication</code> peut être manquante pour le compartiment source.
<code>SrcGetTaggingNotPermitted</code>	S3 sur Outposts n'est pas en mesure d'accéder aux informations de balises d'objets dans le compartiment source. L'autorisation <code>s3-outposts:GetObjectVersionTagging</code> peut être manquante pour le compartiment source.
<code>SrcHeadObjectNotPermitted</code>	S3 sur Outposts n'est pas en mesure de récupérer les métadonnées d'objets du compartiment source. L'autorisation <code>s3-outposts:GetObjectVersionForReplication</code> peut être manquante pour le compartiment source.
<code>SrcObjectNotEligible</code>	L'objet n'est pas éligible à la réplication. L'objet ou ses balises d'objet ne correspondent pas à la configuration de réplication.

Pour plus d'informations sur le dépannage de la réplication, consultez les rubriques suivantes :

- [Création d'un rôle IAM](#)
- [Résolution des problèmes de réplication](#)

Surveillance EventBridge avec CloudWatch

Pour la surveillance, Amazon EventBridge s'intègre à Amazon CloudWatch. EventBridge envoie automatiquement des métriques à CloudWatch chaque minute. Ces mesures incluent le nombre d'[événements](#) auxquels correspond une [règle](#) et le nombre de fois qu'une [cible](#) est invoquée par une

règle. Lorsqu'une règle s'exécute EventBridge, toutes les cibles associées à la règle sont invoquées. Vous pouvez surveiller votre EventBridge comportement de la CloudWatch manière suivante.

- Vous pouvez surveiller les [EventBridgeindicateurs](#) disponibles pour vos EventBridge règles depuis le CloudWatch tableau de bord. Vous pouvez ensuite utiliser des CloudWatch fonctionnalités, telles que les CloudWatch alarmes, pour définir des alarmes sur certains indicateurs. Si ces métriques atteignent les valeurs de seuil personnalisées que vous avez spécifiées dans les alarmes, vous recevez des notifications et pouvez agir en conséquence.
- Vous pouvez définir Amazon CloudWatch Logs comme cible de votre EventBridge règle. Il EventBridge crée ensuite des flux de CloudWatch journaux et Logs stocke le texte des événements sous forme d'entrées de journal. Pour plus d'informations, consultez [EventBridge et CloudWatch Logs](#).

Pour plus d'informations sur le débogage EventBridge de la diffusion et de l'archivage des événements, consultez les rubriques suivantes :

- [Politique relative aux nouvelles tentatives d'événements et utilisation de files d'attente de lettres mortes](#)
- [Archivage des événements EventBridge](#)

Partage de S3 sur Outposts à l'aide de AWS RAM

Simple Storage Service (Amazon S3) sur Outposts prend en charge le partage de la capacité S3 sur plusieurs comptes au sein d'une organisation en utilisant AWS Resource Access Manager ([AWS RAM](#)). Avec le partage de S3 sur Outposts, vous pouvez autoriser d'autres utilisateurs à créer et gérer des compartiments, des points de terminaison et des points d'accès sur votre Outpost.

Cette rubrique montre comment utiliser AWS RAM pour partager S3 sur Outposts et les ressources connexes avec un autre Compte AWS dans votre organisation AWS.

Prérequis

- Le compte propriétaire Outpost dispose d'une organisation configurée dans AWS Organizations. Pour plus d'informations, consultez [Création d'une organisation](#) dans le AWS OrganizationsGuide de l'utilisateur.

- L'organisation comprend le Compte AWS avec lequel vous souhaitez partager votre capacité S3 sur Outposts. Pour de plus amples informations, consultez [Envoi d'invitations à des Comptes AWS](#) dans le Guide de l'utilisateur AWS Organizations.
- Sélectionnez l'une des options suivantes que vous voulez partager. La deuxième ressource (Subnets (Sous-réseaux) ou Outposts) doit être sélectionnée pour que les points de terminaison soient également accessibles. Les points de terminaison sont une exigence liée à la mise en réseau afin d'accéder aux données stockées dans S3 sur Outposts.

Option 1	Option 2
S3 sur Outposts	S3 on Outposts
Permet à l'utilisateur de créer des compartiments sur vos Outposts et points d'accès et d'ajouter des objets à ces compartiments.	Permet à l'utilisateur de créer des compartiments sur vos Outposts et points d'accès et d'ajouter des objets à ces compartiments.
Sous-réseaux	Outposts
Permet à l'utilisateur d'utiliser votre cloud privé virtuel (VPC) et les points de terminaison associés à votre sous-réseau.	Permet à l'utilisateur de voir les diagrammes de capacité S3 et la page d'accueil de la console AWS Outposts. Permet également aux utilisateurs de créer des sous-réseaux sur des Outposts partagés et de créer des points de terminaison.

Procédure

1. Connectez-vous à la AWS Management Console via le Compte AWS propriétaire de l'Outpost, puis ouvrez la console AWS RAM à partir de l'adresse <https://console.aws.amazon.com/ram/home>.
2. Assurez-vous d'avoir activé le partage avec AWS Organizations dans AWS RAM. Pour de plus amples informations, consultez [Activer le partage des ressources dans AWS Organizations](#) dans le Guide de l'utilisateur AWS RAM.
3. Utilisez l'option 1 ou l'option 2 dans les [exigences](#) pour créer un partage de ressources. Si vous disposez de plusieurs ressources S3 sur Outposts, sélectionnez les Amazon Resource Names

(ARN) des ressources que vous souhaitez partager. Pour activer les points de terminaison, partagez votre sous-réseau ou Outpost.

Pour de plus amples informations sur la création d'un partage de ressources, consultez [Créer un partage de ressources](#) dans le AWS RAM Guide de l'utilisateur.

4. Le Compte AWS avec qui vous avez partagé vos ressources devrait maintenant pouvoir utiliser S3 sur Outposts. Selon l'option que vous avez sélectionnée dans les [prérequis](#), fournissez les informations suivantes à l'utilisateur du compte :

Option 1	Option 2
L'ID Outpost	L'ID Outpost
L'ID de VPC	
L'ID de sous-réseau	
L'ID du groupe de sécurité	

Note

L'utilisateur peut confirmer que les ressources ont été partagées avec lui à l'aide de la console AWS RAM, de l'AWS Command Line Interface (AWS CLI), des kits SDK AWS ou de l'API REST. L'utilisateur peut afficher ses partages de ressources existants à l'aide de la commande de l'interface CLI [get-resource-shares](#).

Exemples d'utilisation

Une fois que vous avez partagé vos ressources S3 sur Outposts avec un autre compte, ce compte peut gérer des compartiments et des objets sur votre Outpost. Si vous avez partagé la ressource Subnets (Sous-réseaux), ce compte peut alors utiliser le point de terminaison que vous avez créé. Les exemples suivants montrent comment un utilisateur peut utiliser la AWS CLI pour interagir avec Outpost après avoir partagé ces ressources.

Exemple: Créer un compartiment

L'exemple suivant crée un compartiment nommé *amzn-s3-demo-bucket1* sur l'Outpost *op-01ac5d28a6a232904*. Avant d'utiliser cette commande, remplacez chaque *user input placeholder* par les valeurs appropriées pour votre cas d'utilisation.

```
aws s3control create-bucket --bucket amzn-s3-demo-bucket1 --outpost-id op-01ac5d28a6a232904
```

Pour plus d'informations sur cette commande, consultez [create-bucket](#) dans la Référence de l'AWS CLI.

Exemple: Créer un point d'accès

L'exemple suivant crée un point d'accès sur un Outpost, à l'aide des exemples de paramètre du tableau suivant. Avant d'utiliser cette commande, remplacez ces valeurs *user input placeholder* et le code Région AWS par les valeurs appropriées pour votre cas d'utilisation.

Paramètre	Valeur
ID de compte	<i>111122223333</i>
Nom du point d'accès	<i>example-outpost-access-point</i>
ID Outpost	<i>op-01ac5d28a6a232904</i>
Nom du compartiment Outpost	<i>amzn-s3-demo-bucket1</i>
ID du VPC	<i>vpc-1a2b3c4d5e6f7g8h9</i>

Note

Le paramètre d'ID de compte doit être l'ID Compte AWS du propriétaire du compartiment, qui est l'utilisateur partagé.

```
aws s3control create-access-point --account-id 111122223333 --name example-outpost-access-point \
```

```
--bucket arn:aws:s3-outposts:us-east-1:111122223333:outpost/op-01ac5d28a6a232904/  
bucket/amzn-s3-demo-bucket1 \  
--vpc-configuration VpcId=vpc-1a2b3c4d5e6f7g8h9
```

Pour plus d'informations sur cette commande, consultez [create-access-point](#) dans la Référence de l'AWS CLI.

Exemple: Charger un objet

L'exemple suivant permet de charger le fichier *my_image.jpg* depuis le système de fichiers local de l'utilisateur vers un objet nommé *images/my_image.jpg* via le point d'accès *example-outpost-access-point* sur l'Outpost *op-01ac5d28a6a232904*, détenu par le compte AWS *111122223333*. Avant d'utiliser cette commande, remplacez ces valeurs *user input placeholder* et le code Région AWS par les valeurs appropriées pour votre cas d'utilisation.

```
aws s3api put-object --bucket arn:aws:s3-outposts:us-  
east-1:111122223333:outpost/op-01ac5d28a6a232904/accesspoint/example-outpost-access-  
point \  
--body my_image.jpg --key images/my_image.jpg
```

Pour plus d'informations sur cette commande, consultez [put-object](#) dans la Référence de l'AWS CLI.

Note

Si cette opération aboutit à une erreur de ressource introuvable ou ne répond pas, il se peut que votre VPC n'ait pas de point de terminaison partagé. Pour vérifier s'il existe un point de terminaison partagé, utilisez la commande AWS CLI [list-shared-endpoints](#). S'il n'existe aucun point de terminaison partagé, demandez au propriétaire Outpost de vous en créer un. Pour plus d'informations, consultez [ListSharedEndpoints](#) dans le manuel Amazon Simple Storage Service API Reference.

Exemple: Créer un point de terminaison

L'exemple suivant d'utilisation permet de créer un point de terminaison sur un Outpost partagé. Avant d'utiliser cette commande, remplacez les valeurs *user input placeholder* pour l'ID Outpost, l'ID de sous-réseau et l'ID du groupe de sécurité par les valeurs appropriées pour votre cas d'utilisation.

Note

L'utilisateur ne peut effectuer cette opération que si le partage de ressources comprend la ressource Outposts.

```
aws s3outposts create-endpoint --outposts-id op-01ac5d28a6a232904 --subnet-id XXXXXX --security-group-id XXXXXX
```

Pour plus d'informations sur cette commande, consultez [create-endpoint](#) dans la Référence de l'AWS CLI.

Autres Services AWS qui utilisent S3 sur Outposts

D'autres Services AWS qui s'exécutent localement AWS Outposts peuvent également utiliser la capacité de votre Amazon S3 on Outposts. Dans Amazon, CloudWatch l'espace de S3Outposts noms affiche des métriques détaillées pour les buckets au sein de S3 sur Outposts, mais ces métriques n'incluent pas l'utilisation pour les autres. Services AWS Pour gérer la capacité de S3 on Outposts consommée par d'autres utilisateurs Services AWS, consultez les informations du tableau suivant.

Service AWS	Description	En savoir plus
Amazon S3	Toute utilisation directe de S3 sur Outposts est associée à une métrique de compte et de compartiment CloudWatch correspondante.	Afficher les métriques
Amazon Elastic Block Store (Amazon EBS)	Pour Amazon EBS on Outposts, vous pouvez choisir AWS un Outpost comme destination de capture d'écran et le stocker localement dans votre S3 sur Outpost.	En savoir plus
Amazon Relational Database Service (Amazon RDS)	Vous pouvez utiliser les sauvegardes locales Amazon RDS pour stocker vos sauvegardes RDS localement sur votre Outpost.	En savoir plus

Surveillance de S3 on Outposts

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur APIs les compartiments Outpost que sur les compartiments 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 Command Line Interface (AWS CLI) ou REST. AWS SDKs Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Pour plus d'informations sur la surveillance de votre capacité de stockage Amazon S3 sur Outposts, consultez les rubriques suivantes.

Rubriques

- [Gérer la capacité de S3 on Outposts avec Amazon Metrics CloudWatch](#)
- [Recevoir des notifications d'événements S3 on Outposts à l'aide d'Amazon Events CloudWatch](#)
- [Surveillance de S3 sur les Outposts avec des logs AWS CloudTrail](#)

Gérer la capacité de S3 on Outposts avec Amazon Metrics CloudWatch

Pour vous aider à gérer la capacité S3 fixe de votre Outpost, nous vous recommandons de créer des CloudWatch alertes qui vous avertissent lorsque l'utilisation de votre stockage dépasse un certain seuil. Pour plus d'informations sur les CloudWatch métriques de S3 sur Outposts, consultez [CloudWatch métriques](#). S'il n'y a pas assez d'espace pour stocker un objet sur votre Outpost, l'API renvoie une exemption de capacité insuffisante (ICE). Pour libérer de l'espace, vous pouvez créer des CloudWatch alarmes qui déclenchent la suppression explicite des données ou utiliser une politique d'expiration du cycle de vie pour faire expirer les objets. Pour enregistrer les données avant de les supprimer, vous pouvez AWS DataSync les utiliser pour copier les données de votre compartiment Amazon S3 on Outposts vers un compartiment S3 dans un. Région AWS Pour plus

d'informations sur l'utilisation DataSync, voir [Getting Started with AWS DataSync](#) dans le guide de AWS DataSync l'utilisateur.

CloudWatch métriques

L'espace de noms `S3Outposts` inclut les métriques suivantes pour les compartiments Amazon S3 sur Outposts. Vous pouvez surveiller le nombre total d'octets S3 sur Outposts alloués, le nombre total d'octets libres disponibles pour les objets et la taille totale de tous les objets pour un compartiment donné. Des métriques liées aux compartiments ou aux comptes existent pour toute utilisation directe de S3. L'utilisation indirecte de S3, telle que le stockage d'instantanés locaux Amazon Elastic Block Store ou de sauvegardes Amazon Relational Database Service sur un Outpost, consomme de la capacité S3, mais n'est pas incluse dans les métriques liées aux compartiments ou aux comptes. Pour plus d'informations sur les instantanés locaux Amazon EBS, consultez [Instantanés locaux Amazon EBS sur Outposts](#). Pour consulter votre rapport de coûts Amazon EBS, rendez-vous <https://console.aws.amazon.com/costmanagement/> sur.

Note

S3 on Outposts ne prend en charge que les métriques suivantes et aucune autre métrique Amazon S3.

S3 on Outposts ayant une limite de capacité fixe, nous vous recommandons de créer des CloudWatch alarmes pour vous avertir lorsque l'utilisation de votre stockage dépasse un certain seuil.

Métrique	Description	Période	Unités	Type
OutpostTotalBytes	Capacité totale allouée en octets pour un Outpost	5 minutes	Octets	S3 sur Outposts
OutpostFreeBytes	Nombre d'octets libres disponibles sur un Outpost pour stocker les données des clients.	5 minutes	Octets	S3 sur Outposts
BucketUsedBytes	Taille totale de tous les objets pour le compartiment donné.	5 minutes	Octets	S3 sur Outposts. Utilisation directe de S3 uniquement.

Métrique	Description	Période	Unités	Type
AccountTotalBytes	Taille totale de tous les objets pour le compte Outposts spécifié.	5 minutes	Octets	S3 sur Outposts. Utilisation directe de S3 uniquement.
BytesPendingReplication	Nombre total d'octets d'objets en attente de réplication pour une règle de réplication donnée. Pour plus d'informations sur l'activation des métriques de réplication, consultez la section Creating replication rules between Outposts (Création de règles de réplication entre Outposts).	5 minutes	Octets	Facultatif. Pour la réplication S3 sur Outposts.
OperationsPendingReplication	Nombre total d'opérations en attente de réplication pour une règle de réplication donnée. Pour plus d'informations sur l'activation des métriques de réplication, consultez la section Creating replication rules between Outposts (Création de règles de réplication entre Outposts).	5 minutes	Comptes	Facultatif. Pour la réplication S3 sur Outposts.

Métrique	Description	Période	Unités	Type
Replica onLatenc	Nombre actuel de secondes de retard entre le compartiment de destination de réplication et le compartiment source pour une règle de réplication donnée. Pour plus d'informations sur l'activation des métriques de réplication, consultez la section Creating replication rules between Outposts (Création de règles de réplication entre Outposts).	5 minutes	Secondes	Facultatif. Pour la réplication S3 sur Outposts.

Recevoir des notifications d'événements S3 on Outposts à l'aide d'Amazon Events CloudWatch

Vous pouvez utiliser CloudWatch Events pour créer une règle pour tout événement d'API Amazon S3 on Outposts. Lorsque vous créez une règle, vous pouvez choisir d'être averti via toutes les CloudWatch cibles prises en charge, notamment Amazon Simple Queue Service (Amazon SQS), Amazon Simple Notification Service (Amazon SNS) et AWS Lambda. Pour plus d'informations, consultez la liste des [AWS services pouvant être la cible d' CloudWatch événements](#) dans le guide de l'utilisateur Amazon CloudWatch Events. Pour choisir un service cible qui fonctionnera avec votre S3 sur Outposts, consultez la section [Création d'une règle d' CloudWatch événements qui se déclenche lors d'un appel d' AWS API AWS CloudTrail](#) dans le guide de l'utilisateur Amazon CloudWatch Events.

Note

Pour les opérations d'objets S3 on Outposts, les événements d'appel d' AWS API envoyés par S3 ne CloudTrail respecteront vos règles que si vous avez configuré des pistes (éventuellement avec des sélecteurs d'événements) pour recevoir ces événements. Pour plus d'informations, consultez la section [Utilisation des fichiers CloudTrail journaux](#) dans le Guide de AWS CloudTrail l'utilisateur.

Exemple

Voici un exemple de règle pour l'opération `DeleteObject`. Pour utiliser cet exemple de règle, remplacez *amzn-s3-demo-bucket1* par le nom de votre compartiment S3 sur Outposts.

```
{
  "source": [
    "aws.s3-outposts"
  ],
  "detail-type": [
    "AWS API call through CloudTrail"
  ],
  "detail": {
    "eventSource": [
      "s3-outposts.amazonaws.com"
    ],
    "eventName": [
      "DeleteObject"
    ],
    "requestParameters": {
      "bucketName": [
        "amzn-s3-demo-bucket1"
      ]
    }
  }
}
```

Surveillance de S3 sur les Outposts avec des logs AWS CloudTrail

Amazon S3 on Outposts est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions effectuées par un utilisateur, un rôle ou un utilisateur Service AWS dans S3 sur Outposts. Vous pouvez utiliser AWS CloudTrail pour obtenir des informations sur des demandes au niveau du compartiment et au niveau de l'objet sur S3 sur Outposts pour auditer et journaliser votre activité d'événements S3 sur Outposts.

[Pour activer les événements de CloudTrail données pour tous vos compartiments Outposts ou pour une liste de compartiments Outposts spécifiques, vous devez créer un suivi manuellement dans CloudTrail](#) Pour plus d'informations sur les entrées de fichiers CloudTrail journaux, consultez [S3 sur les entrées de fichiers journaux d'Outposts](#).

Pour obtenir la liste complète des événements CloudTrail liés aux données pour S3 on Outposts, consultez la section [Événements relatifs aux données Amazon S3 CloudTrail dans](#) le guide de l'utilisateur Amazon S3.

Note

- Il est recommandé de créer une politique de cycle de vie pour votre bucket Outposts d'événements de AWS CloudTrail données. Configurez la politique de cycle de vie pour supprimer périodiquement les fichiers journaux après le délai à l'issue duquel vous devez les auditer. Cela permet de réduire la quantité de données analysées par Amazon Athena pour chaque requête. Pour de plus amples informations, veuillez consulter [Création et gestion d'une configuration de cycle de vie pour votre compartiment Amazon S3 on Outposts](#).
- 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 CloudTrail journalisation des objets dans un compartiment S3 on Outposts


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 Amazon S3 on Outposts. CloudTrail prend en charge la journalisation de S3 sur les opérations d'API au niveau des objets d'Outposts, telles `GetObject` que, et. `DeleteObject` `PutObject` Ces événements sont des événements de données.

Par défaut, les CloudTrail sentiers n'enregistrent pas les événements liés aux données. Cependant, vous pouvez configurer des journaux de suivi pour consigner les événements de données pour les compartiments S3 sur Outposts que vous spécifiez ou pour consigner les événements de données pour tous les compartiments S3 sur Outposts dans votre Compte AWS.

CloudTrail ne renseigne pas les événements de données dans l'historique des CloudTrail événements. De plus, les opérations d'API S3 on Outposts au niveau du bucket ne sont pas toutes renseignées dans l'historique des événements. CloudTrail Pour plus d'informations sur la manière d'interroger CloudTrail les journaux, consultez les [sections Utilisation CloudWatch des modèles](#)


[de filtrage Amazon Logs et Amazon Athena pour interroger les CloudTrail journaux](#) dans le AWS Knowledge Center.

Pour configurer un journal de suivi afin de journaliser les événements de données pour un compartiment S3 sur Outposts, vous pouvez utiliser la console AWS CloudTrail ou la console Amazon S3. Si vous configurez un journal pour consigner les événements de données pour tous les compartiments S3 on Outposts de vos compartiments Compte AWS, il est plus facile d'utiliser la console. CloudTrail Pour plus d'informations sur l'utilisation de la CloudTrail console pour configurer un journal des événements de données S3 on Outposts, consultez la section Événements liés aux [données dans le guide](#) de l'AWS CloudTrail 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 on Outposts.

 Note

La personne Compte AWS qui crée le compartiment en est propriétaire et est la seule à pouvoir configurer les événements de données S3 on Outposts à envoyer. AWS CloudTrail

Pour activer la journalisation des événements de CloudTrail données pour les objets d'un bucket S3 on Outposts

1. 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 Outposts buckets (Compartiments Outposts).
3. Choisissez le nom du bucket Outposts dont vous souhaitez enregistrer les événements de données en utilisant. CloudTrail
4. Choisissez Propriétés.
5. Dans la section AWS CloudTrail des événements de données, choisissez Configurer dans CloudTrail.

La AWS CloudTrail console s'ouvre.

Vous pouvez créer une nouvelle CloudTrail piste ou réutiliser une piste existante et configurer les événements de données S3 on Outposts pour qu'ils soient enregistrés dans votre trace.

6. Sur la page du tableau de bord de la CloudTrail console, choisissez Create trail.
7. Sur la page Étape 1 Choisir les attributs du journal de suivi, donnez un nom au journal de suivi, choisissez un compartiment S3 pour stocker les journaux de suivi, spécifiez les autres paramètres souhaités, puis cliquez sur Suivant.
8. Sur la page Étape 2 Choisir des événements de journaux, sous Type d'événement, choisissez Événements de données.

Pour Type d'événement de données, choisissez S3 Outposts. Choisissez Suivant.

Note

- Lorsque vous créez un journal de suivi et que vous configurez la journalisation des événements de données pour S3 sur Outposts, vous devez spécifier correctement le type d'événement de données.
- Si vous utilisez la CloudTrail console, choisissez le type d'événement S3 Outposts for Data. 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 S3 on Outposts dans la CloudTrail console, consultez la section [Journalisation des événements de données pour les objets Amazon S3](#) dans le guide de l'AWS CloudTrail utilisateur.
- Si vous utilisez le AWS Command Line Interface (AWS CLI) ou le AWS SDKs, définissez le `resources.type` champ sur `AWS::S3Outposts::Object`. Pour plus d'informations sur la façon de consigner les événements de données S3 on Outposts avec le AWS CLI, consultez la section [Log S3 on Outposts dans le guide de l'utilisateur](#).AWS CloudTrail
- Si vous utilisez la CloudTrail console ou la console Amazon S3 pour configurer un journal des événements de données pour un compartiment S3 on Outposts, la console Amazon S3 indique que la journalisation au niveau des objets est activée pour le compartiment.

9. Sur la page Étape 3 Vérifier et créer, passez en revue les attributs du suivi et les événements du journal que vous avez configurés. Choisissez ensuite Créer un journal de suivi.

Pour désactiver la journalisation des événements de CloudTrail données pour les objets d'un bucket S3 on Outposts

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 volet 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 S3 sur Outposts.
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.

Entrées du fichier AWS CloudTrail journal d'Amazon S3 on Outposts

Les événements de gestion d'Amazon S3 on Outposts sont disponibles via. AWS CloudTrail En outre, vous pouvez éventuellement [activer la journalisation des événements de données dans AWS CloudTrail](#).

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment S3 dans une région que vous spécifiez. CloudTrail les journaux de vos compartiments Outposts incluent un nouveau champ `deviceDetails`, qui identifie l'Outpost où se trouve le bucket spécifié.

Les champs de journal supplémentaires incluent l'action demandée, la date et l'heure de l'action, ainsi que les paramètres de la demande. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant une [PutObject](#) sur s3-outposts.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "111122223333",
```

```

    "arn": "arn:aws:iam::111122223333:user/yourUserName",
    "accountId": "222222222222",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "yourUserName"
  },
  "eventTime": "2020-11-30T15:44:33Z",
  "eventSource": "s3-outposts.amazonaws.com",
  "eventName": "PutObject",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "26.29.66.20",
  "userAgent": "aws-cli/1.18.39 Python/3.4.10 Darwin/18.7.0 botocore/1.15.39",
  "requestParameters": {
    "expires": "Wed, 21 Oct 2020 07:28:00 GMT",
    "Content-Language": "english",
    "x-amz-server-side-encryption-customer-key-MD5": "wJa1rXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ObjectCannedACL": "BucketOwnerFullControl",
    "x-amz-server-side-encryption": "Aes256",
    "Content-Encoding": "gzip",
    "Content-Length": "10",
    "Cache-Control": "no-cache",
    "Content-Type": "text/html; charset=UTF-8",
    "Content-Disposition": "attachment",
    "Content-MD5": "je7MtGbClwBF/2Zp9Utk/h3yCo8nvbEXAMPLEKEY",
    "x-amz-storage-class": "Outposts",
    "x-amz-server-side-encryption-customer-algorithm": "Aes256",
    "bucketName": "amzn-s3-demo-bucket1",
    "Key": "path/upload.sh"
  },
  "responseElements": {
    "x-amz-server-side-encryption-customer-key-MD5": "wJa1rXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "x-amz-server-side-encryption": "Aes256",
    "x-amz-version-id": "001",
    "x-amz-server-side-encryption-customer-algorithm": "Aes256",
    "ETag": "d41d8cd98f00b204e9800998ecf8427f"
  },
  "additionalEventData": {
    "CipherSuite": "ECDHE-RSA-AES128-SHA",
    "bytesTransferredIn": 10,
    "x-amz-id-2": "29xXQBV20
+x0HKItvzY1suLv1i6A52E0z0X159fpfsItYd58JhXwKxXAXI4IQkp6",
    "SignatureVersion": "SigV4",
    "bytesTransferredOut": 20,

```

```
    "AuthenticationMethod": "AuthHeader"
  },
  "requestID": "8E96D972160306FA",
  "eventID": "ee3b4e0c-ab12-459b-9998-0a5a6f2e4015",
  "readOnly": false,
  "resources": [
    {
      "accountId": "222222222222",
      "type": "AWS::S3Outposts::Object",
      "ARN": "arn:aws:s3-outposts:us-east-1:YYY:outpost/op-01ac5d28a6a232904/
bucket/path/upload.sh"
    },
    {
      "accountId": "222222222222",
      "type": "AWS::S3Outposts::Bucket",
      "ARN": "arn:aws:s3-outposts:us-east-1:YYY:outpost/op-01ac5d28a6a232904/
bucket/"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": false,
  "recipientAccountId": "444455556666",
  "sharedEventID": "02759a4c-c040-4758-b84b-7cbaaf17747a",
  "edgeDeviceDetails": {
    "type": "outposts",
    "deviceId": "op-01ac5d28a6a232904"
  },
  "eventCategory": "Data"
}
```

Développement avec Amazon S3 on Outposts

Avec Amazon S3 on Outposts, vous pouvez créer des compartiments S3 sur vos AWS Outposts 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. S3 on Outposts fournit une nouvelle classe de stockage, S3 Outposts (OUTPOSTS), qui utilise Amazon S3 APIs et est conçue pour stocker des données de manière durable et redondante sur plusieurs appareils et serveurs de votre entreprise. AWS Outposts Vous communiquez avec votre compartiment Outpost à l'aide d'un point d'accès et d'une connexion de point de terminaison via un cloud privé virtuel (VPC). Vous pouvez utiliser les mêmes fonctionnalités sur APIs les compartiments Outpost que sur les compartiments 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 Command Line Interface (AWS CLI) ou REST. AWS SDKs Pour de plus amples informations, consultez [Qu'est-ce que Amazon S3 sur Outposts ?](#).

Les rubriques suivantes fournissent des informations sur le développement avec S3 on Outposts.

Rubriques

- [Régions dans lesquelles S3 sur Outposts est pris en charge](#)
- [Opérations d'API Amazon S3 on Outposts](#)
- [Configurer les client de contrôle S3 pour S3 on Outposts à l'aide du kit SDK pour Java](#)
- [Envoyer des requêtes à S3 sur Outposts over IPv6](#)

Régions dans lesquelles S3 sur Outposts est pris en charge

S3 sur Outposts est pris en charge dans les Régions AWS suivantes.

- 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)
- Afrique (Le Cap) (af-south-1)
- Asie-Pacifique (Jakarta) (ap-southeast-3)
- Asie-Pacifique (Mumbai) (ap-south-1)

- Asie-Pacifique (Osaka) (ap-northeast-3)
- 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)
- Europe (Francfort) (eu-central-1)
- Europe (Irlande) (eu-west-1)
- Europe (Londres) (eu-west-2)
- Europe (Milan) (eu-south-1)
- Europe (Paris) (eu-west-3)
- Europe (Stockholm) (eu-north-1)
- Israël (Tel Aviv) (il-central-1)
- Moyen-Orient (Bahreïn) (me-south-1)
- Amérique du Sud (São Paulo) (sa-east-1)
- AWS GovCloud (US-Est) (us-gov-east-1)
- AWS GovCloud (US-West) (us-gov-west-1)

Opérations d'API Amazon S3 on Outposts

Cette rubrique répertorie les opérations d'API Amazon S3, Amazon S3 Control et Amazon S3 on Outposts que vous pouvez utiliser avec Amazon S3 on Outposts.

Rubriques

- [Opérations d'API Amazon S3 pour la gestion des objets](#)
- [Opérations d'API de contrôle Amazon S3 pour la gestion des compartiments](#)
- [Opérations d'API S3 sur Outposts pour la gestion d'Outposts](#)

Opérations d'API Amazon S3 pour la gestion des objets

S3 on Outposts est conçu pour utiliser les mêmes opérations d'API sur les objets qu'Amazon S3. Vous devez utiliser des points d'accès pour accéder à tout objet dans un compartiment Outpost.

Lorsque vous utilisez une opération d'API d'objet avec S3 sur Outposts, vous fournissez l'Amazon Resource Name (ARN) du point d'accès Outposts ou l'alias de point d'accès. Pour plus d'informations sur les alias de point d'accès, consultez [Utilisation d'un alias de type compartiment pour le point d'accès de votre compartiment S3 sur Outposts](#).

Amazon S3 on Outposts prend en charge les opérations suivantes d'API Amazon S3 :

- [AbortMultipartUpload](#)
- [CompleteMultipartUpload](#)
- [CopyObject](#)
- [CreateMultipartUpload](#)
- [DeleteObject](#)
- [DeleteObjects](#)
- [DeleteObjectTagging](#)
- [GetObject](#)
- [GetObjectTagging](#)
- [HeadBucket](#)
- [HeadObject](#)
- [ListMultipartUploads](#)
- [ListObjects](#)
- [ListObjectsV2](#)
- [ListObjectVersions](#)
- [ListParts](#)
- [PutObject](#)
- [PutObjectTagging](#)
- [UploadPart](#)
- [UploadPartCopy](#)

Opérations d'API de contrôle Amazon S3 pour la gestion des compartiments

S3 on Outposts prend en charge les opérations d'API de contrôle Amazon S3 suivantes pour une utilisation avec les compartiments.

- [CreateAccessPoint](#)

- [CreateBucket](#)
- [DeleteAccessPoint](#)
- [DeleteAccessPointPolicy](#)
- [DeleteBucket](#)
- [DeleteBucketLifecycleConfiguration](#)
- [DeleteBucketPolicy](#)
- [DeleteBucketReplication](#)
- [DeleteBucketTagging](#)
- [GetAccessPoint](#)
- [GetAccessPointPolicy](#)
- [GetBucket](#)
- [GetBucketLifecycleConfiguration](#)
- [GetBucketPolicy](#)
- [GetBucketReplication](#)
- [GetBucketTagging](#)
- [GetBucketVersioning](#)
- [ListAccessPoints](#)
- [ListRegionalBuckets](#)
- [PutAccessPointPolicy](#)
- [PutBucketLifecycleConfiguration](#)
- [PutBucketPolicy](#)
- [PutBucketReplication](#)
- [PutBucketTagging](#)
- [PutBucketVersioning](#)

Opérations d'API S3 sur Outposts pour la gestion d'Outposts

S3 on Outposts prend en charge les opérations d'API Amazon S3 on Outposts suivantes pour la gestion des points de terminaison.

- [CreateEndpoint](#)
- [DeleteEndpoint](#)

- [ListEndpoints](#)
- [ListOutpostsWithS3](#)
- [ListSharedEndpoints](#)

Configurer les client de contrôle S3 pour S3 on Outposts à l'aide du kit SDK pour Java

L'exemple suivant illustre la configuration du client de contrôle Amazon S3 pour S3 on Outposts à l'aide du AWS SDK pour Java. Pour utiliser cet exemple, remplacez chaque *user input placeholder* par vos propres informations.

```
import com.amazonaws.auth.AWSStaticCredentialsProvider;
import com.amazonaws.auth.BasicAWSCredentials;
import com.amazonaws.services.s3control.AWSS3Control;
import com.amazonaws.services.s3control.AWSS3ControlClient;

public AWSS3Control createS3ControlClient() {

    String accessKey = AWSAccessKey;
    String secretKey = SecretAccessKey;
    BasicAWSCredentials awsCreds = new BasicAWSCredentials(accessKey, secretKey);

    return AWSS3ControlClient.builder().enableUseArnRegion()
        .withCredentials(new AWSStaticCredentialsProvider(awsCreds))
        .build();
}
```

Envoyer des requêtes à S3 sur Outposts over IPv6

Les points de terminaison à double pile Amazon S3 on Outposts et S3 on Outposts prennent en charge les demandes adressées aux compartiments S3 on Outposts en utilisant le protocole or. IPv6 IPv4 Grâce à la prise en IPv6 charge de S3 on Outposts, vous pouvez accéder à vos buckets et aux ressources de votre plan de contrôle et les exploiter via S3 on Outposts sur les réseaux. APIs IPv6

Note

Les [actions d'objets S3 on Outposts](#) (telles que PutObject ou GetObject) ne sont pas prises en charge sur IPv6 les réseaux.

Il n'y a pas de frais supplémentaires pour accéder à S3 sur les Outposts via IPv6 les réseaux. Pour plus d'informations sur S3 sur Outposts, consultez [Tarification S3 sur Outposts](#).

Rubriques

- [Commencer avec IPv6](#)
- [Utilisation de points de terminaison à double pile pour effectuer des demandes sur un réseau IPv6](#)
- [Utilisation des IPv6 adresses dans les politiques IAM](#)
- [Test de compatibilité d'adresses IP](#)
- [Utilisation IPv6 avec AWS PrivateLink](#)
- [Utilisation de points de terminaison à double pile S3 sur Outposts](#)

Commencer avec IPv6

Pour envoyer une demande à un compartiment S3 on Outposts IPv6, vous devez utiliser un point de terminaison à double pile. La section suivante décrit comment effectuer des demandes à l'aide de points IPv6 de terminaison à double pile.

Les points suivants sont importants à prendre en compte avant d'essayer d'accéder à un bucket S3 on Outposts : IPv6

- Le client et le réseau accédant au compartiment doivent être autorisés à utiliser le protocole IPv6.
- Les demandes d'accès de type hébergé virtuel et de style chemin sont prises en charge. IPv6 Pour de plus amples informations, veuillez consulter [Utilisation de points de terminaison à double pile S3 sur Outposts](#).
- Si vous utilisez le filtrage des adresses IP source dans votre utilisateur Gestion des identités et des accès AWS (IAM) ou les politiques du bucket S3 on Outposts, vous devez mettre à jour les politiques pour IPv6 inclure les plages d'adresses.

Note

Cette exigence s'applique uniquement aux opérations du bucket S3 on Outposts et aux ressources du plan de contrôle sur IPv6 les réseaux. Les actions d'[objets Amazon S3 on Outposts ne sont pas prises](#) en charge sur tous les réseaux IPv6 .

- Lors de l'utilisation IPv6, les fichiers journaux d'accès au serveur génèrent les adresses IP dans un IPv6 format donné. Vous devez mettre à jour les outils, scripts et logiciels existants que vous utilisez pour analyser les fichiers journaux S3 on Outposts, afin qu'ils puissent analyser les adresses IP distantes IPv6 formatées. Les outils, scripts et logiciels mis à jour analyseront ensuite correctement les adresses IP distantes IPv6 formatées.

Utilisation de points de terminaison à double pile pour effectuer des demandes sur un réseau IPv6

Pour effectuer des requêtes avec S3 on Outposts via des appels d'API IPv6, vous pouvez utiliser des points de terminaison à double pile via le SDK. AWS CLI AWS Les opérations de l'[API de contrôle Amazon S3 et les opérations de l'API S3 on Outposts](#) fonctionnent de la même manière, que vous accédez à S3 on Outposts via un protocole ou un IPv6 protocole. IPv4 Sachez toutefois que les [actions d'objets S3 on Outposts](#) (telles que PutObject ouGetObject) ne sont pas prises en charge sur IPv6 les réseaux.

Lorsque vous utilisez le AWS Command Line Interface (AWS CLI) et AWS SDKs, vous pouvez utiliser un paramètre ou un indicateur pour passer à un point de terminaison à double pile. Vous pouvez également spécifier directement le point de terminaison à double pile pour remplacer le point de terminaison S3 sur Outposts dans le fichier de configuration.

Vous pouvez utiliser un point de terminaison à double pile pour accéder à un bucket S3 on Outposts IPv6 depuis l'un des sites suivants :

- Le AWS CLI, tu vois [En utilisant des points de terminaison à double pile à partir du AWS CLI](#).
- Le AWS SDKs, tu vois [Utilisation de S3 sur les points de terminaison à double pile d'Outposts à partir du AWS SDKs](#).

Utilisation des IPv6 adresses dans les politiques IAM

Avant d'essayer d'accéder à un bucket S3 on Outposts à l'aide d'un IPv6 protocole, assurez-vous que les politiques de bucket des utilisateurs IAM ou S3 on Outposts utilisées pour le filtrage des adresses IP sont mises à jour pour inclure les plages d'adresses IPv6. Si les politiques de filtrage des adresses IP ne sont pas mises à jour pour gérer IPv6 les adresses, vous risquez de perdre l'accès à un bucket S3 on Outposts lorsque vous essayez d'utiliser le IPv6 protocole.

Les politiques IAM qui filtrent les adresses IP utilisent des [opérateurs de condition d'adresse IP](#). La politique de compartiment S3 on Outposts suivante identifie la plage d'adresses IP 54.240.143.* d'IPv4 adresses autorisées à l'aide d'opérateurs de condition d'adresse IP. Toute adresse IP hors de cette plage se verra refuser l'accès au compartiment S3 sur Outposts (DOC-EXAMPLE-BUCKET). Comme toutes les IPv6 adresses se situent en dehors de la plage autorisée, cette politique empêche IPv6 les adresses d'y accéder DOC-EXAMPLE-BUCKET.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IPAllow",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3-outposts:*",
      "Resource": "arn:aws:s3-outposts:us-east-1:111122223333:outpost/OUTPOSTS-ID/bucket/DOC-EXAMPLE-BUCKET/*",
      "Condition": {
        "IpAddress": {
          "aws:SourceIp": "54.240.143.0/24"
        }
      }
    }
  ]
}
```

Vous pouvez modifier l'élément `Condition` de la politique de compartiment S3 on Outposts pour autoriser à la fois les plages d'adresses IPv4 (54.240.143.0/24) et IPv6 (2001:DB8:1234:5678::/64), comme indiqué dans l'exemple suivant. Vous pouvez utiliser le

même type de bloc Condition que celui indiqué dans l'exemple pour mettre à jour vos stratégies de compartiment et d'utilisateur IAM.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": [
      "54.240.143.0/24",
      "2001:DB8:1234:5678::/64"
    ]
  }
}
```

Avant de l'utiliser, IPv6 vous devez mettre à jour toutes les politiques pertinentes relatives aux utilisateurs et aux compartiments IAM qui utilisent le filtrage des adresses IP pour autoriser les plages d' IPv6 adresses. Nous vous recommandons de mettre à jour vos politiques IAM avec les plages d' IPv6 adresses de votre organisation en plus de vos plages d' IPv4 adresses existantes. Pour un exemple de politique de compartiment qui autorise l'accès IPv6 aux deux IPv4, voir [Restriction de l'accès à des adresses IP spécifiques](#).

Vous pouvez consulter vos politiques utilisateur IAM à l'aide de la console IAM à l'adresse. <https://console.aws.amazon.com/iam/> Pour de plus amples informations sur IAM, consultez le [Guide de l'utilisateur IAM](#). Pour en savoir plus sur la modification des politiques de compartiments S3 sur Outposts, consultez [Ajout ou modification d'une politique de compartiment pour un compartiment Amazon S3 on Outposts](#).

Test de compatibilité d'adresses IP

Si vous utilisez une instance Linux ou Unix, ou une plateforme macOS X, vous pouvez tester votre accès à un point de terminaison à double pile. IPv6 Par exemple, pour tester la connexion à Amazon S3 sur les points de terminaison Outposts IPv6, utilisez la commande suivante : dig

```
dig s3-outposts.us-west-2.api.aws AAAA +short
```

Si votre point de terminaison à double pile sur un IPv6 réseau est correctement configuré, la dig commande renvoie les IPv6 adresses connectées. Par exemple :

```
dig s3-outposts.us-west-2.api.aws AAAA +short

2600:1f14:2588:4800:b3a9:1460:159f:ebce
```

```
2600:1f14:2588:4802:6df6:c1fd:ef8a:fc76
```

```
2600:1f14:2588:4801:d802:8ccf:4e04:817
```

Utilisation IPv6 avec AWS PrivateLink

S3 on Outposts prend en charge le IPv6 protocole pour les AWS PrivateLink services et les points de terminaison. Grâce à la prise en charge du IPv6 protocole, vous pouvez vous connecter aux points de terminaison de service au sein de votre VPC via des réseaux, à partir de connexions IPv6 sur site ou d'autres connexions privées. La prise en charge [AWS PrivateLink de S3 on Outposts](#) vous permet également d'intégrer des points de terminaison AWS PrivateLink à double pile. Pour savoir comment l'activer IPv6 AWS PrivateLink, consultez [Accélérez votre IPv6 adoption grâce AWS PrivateLink aux services et aux terminaux](#).

Note

Pour mettre à jour le type d'adresse IP pris en charge de IPv4 à IPv6, voir [Modifier le type d'adresse IP pris en charge](#) dans le Guide de AWS PrivateLink l'utilisateur.

Utilisation IPv6 avec AWS PrivateLink

Si vous utilisez AWS PrivateLink avec IPv6, vous devez créer un point de terminaison d'IPv6 interface VPC ou à double pile. Pour connaître les étapes générales de création d'un point de terminaison VPC à l'aide du AWS Management Console, consultez la section [Accès à un AWS service à l'aide d'un point de terminaison VPC d'interface](#) dans le guide de l'utilisateur AWS PrivateLink.

AWS Management Console

Utilisez la procédure suivante pour créer un point de terminaison de VPC d'interface qui se connecte à S3 sur Outposts.

1. Connectez-vous à la console VPC AWS Management Console et ouvrez-la à l'adresse. <https://console.aws.amazon.com/vpc/>
2. Dans le panneau de navigation, choisissez Points de terminaison.
3. Choisissez Créer un point de terminaison.
4. Pour Service category (Catégorie de service), choisissez Services AWS .

5. Pour Nom du service, choisissez le service S3 sur Outposts (com.amazonaws.us-east-1.s3-outposts).
6. Pour VPC, choisissez le VPC à partir duquel vous accédez à S3 sur Outposts.
7. Pour Sous-réseaux, choisissez un sous-réseau unique par zone de disponibilité, à partir duquel vous accédez à S3 sur Outposts. Il n'est pas possible de sélectionner plusieurs sous-réseaux dans la même zone de disponibilité. Pour chaque sous-réseau que vous sélectionnez, une nouvelle interface réseau du point de terminaison est créée. Par défaut, les adresses IP figurant dans les plages d'adresses IP des sous-réseaux sont affectées aux interfaces réseau des points de terminaison. Pour désigner une adresse IP pour une interface réseau de point de terminaison, choisissez Designate IP addresses et entrez une IPv6 adresse dans la plage d'adresses de sous-réseau.
8. Pour Type d'adresse IP, choisissez Double pile. Attribuez à la fois IPv6 des adresses IPv4 et des adresses aux interfaces réseau de vos terminaux. Cette option n'est prise en charge que si tous les sous-réseaux sélectionnés possèdent à la fois des plages d' IPv6 adresses IPv4 et des plages d'adresses.
9. Pour Groupes de sécurité, choisissez les groupes de sécurité à associer aux interfaces réseau du point de terminaison pour le point de terminaison de VPC. Par défaut, le groupe de sécurité par défaut est associé au VPC.
10. 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. Cette option n'est disponible que si le service prend en charge les politiques de points de terminaison de VPC. Pour plus d'informations, consultez [Politiques de point de terminaison](#).
11. (Facultatif) Pour ajouter une balise, choisissez Ajouter une nouvelle balise et entrez la clé et la valeur de la balise.
12. Choisissez Créer un point de terminaison.

Exemple– Politique de compartiments S3 sur Outposts

Pour permettre à S3 sur Outposts d'interagir avec vos points de terminaison de VPC, vous pouvez ensuite mettre à jour votre politique S3 sur Outposts comme suit :

```
{
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "s3-outposts:*",  
    "Resource": "*",  
    "Principal": "*"   
  }  
]
```

AWS CLI

Note

Pour activer le IPv6 réseau sur le point de terminaison de votre VPC, vous devez avoir IPv6 défini le SupportedIpAddressType filtre pour S3 sur les Outposts.

L'exemple suivant utilise la commande `create-vpc-endpoint` pour créer un nouveau point de terminaison d'interface à double pile.

```
aws ec2 create-vpc-endpoint \  
--vpc-id vpc-12345678 \  
--vpc-endpoint-type Interface \  
--service-name com.amazonaws.us-east-1.s3-outposts \  
--subnet-id subnet-12345678 \  
--security-group-id sg-12345678 \  
--ip-address-type dualstack \  
--dns-options "DnsRecordIpType=dualstack"
```

Selon la configuration du AWS PrivateLink service, les connexions de point de terminaison nouvellement créées devront peut-être être acceptées par le fournisseur de services de point de terminaison VPC avant de pouvoir être utilisées. Pour plus d'informations, consultez [Accepter et rejeter les demandes de connexion de point de terminaison](#) dans le Guide de l'utilisateur AWS PrivateLink .

L'exemple suivant utilise la `modify-vpc-endpoint` commande pour mettre à jour le point de terminaison VPC IPv -only vers un point de terminaison à double pile. Le point de terminaison à double pile permet d'accéder à la fois aux IPv6 réseaux IPv4 et.

```
aws ec2 modify-vpc-endpoint \  
--vpc-endpoint-id vpce-12345678 \  
--add-subnet-ids subnet-12345678 \  
--remove-subnet-ids subnet-12345678 \  
--ip-address-type dualstack \  
--dns-options "DnsRecordIpType=dualstack"
```

Pour plus d'informations sur la manière d'activer le IPv6 réseau pour AWS PrivateLink, consultez [Accélérez votre IPv6 adoption grâce AWS PrivateLink aux services et aux terminaux](#).

Utilisation de points de terminaison à double pile S3 sur Outposts

Les points de terminaison à double pile S3 on Outposts prennent en charge les demandes adressées à S3 on Outposts sur et. IPv6 IPv4 Cette section décrit comment utiliser les points de terminaison à double pile S3 sur Outposts.

Rubriques

- [Points de terminaison à double pile S3 sur Outposts](#)
- [En utilisant des points de terminaison à double pile à partir du AWS CLI](#)
- [Utilisation de S3 sur les points de terminaison à double pile d'Outposts à partir du AWS SDKs](#)

Points de terminaison à double pile S3 sur Outposts

Lorsque vous envoyez une demande à un point de terminaison à double pile, l'URL du compartiment S3 on Outposts est convertie en adresse ou IPv6 IPv4 en adresse. Pour plus d'informations sur l'accès à un bucket S3 on Outposts via IPv6, consultez. [Envoyer des requêtes à S3 sur Outposts over IPv6](#)


Pour accéder à un compartiment S3 sur Outposts via un point de terminaison à double pile, utilisez un nom de point de terminaison de type chemin. S3 sur Outposts prend uniquement en charge les noms des points de terminaison à double pile régionaux, ce qui signifie que vous devez spécifier la région dans le nom.

Pour un point de FIPs terminaison de type chemin à double pile, utilisez la convention de dénomination suivante :

```
s3-outposts-fips.region.api.aws
```

Pour un point de terminaison non FIPS à double pile, utilisez la convention de dénomination suivante :

```
s3-outposts.region.api.aws
```

 Note

Les noms des points de terminaison de type hébergement virtuel ne sont pas pris en charge dans S3 sur Outposts.

En utilisant des points de terminaison à double pile à partir du AWS CLI

Cette section fournit des exemples de AWS CLI commandes utilisées pour envoyer des demandes à un point de terminaison à double pile. Pour obtenir des instructions sur la configuration du AWS CLI, voir [Commencer à utiliser le SDK AWS CLI and pour Java](#).

Vous définissez la valeur de configuration `use_dualstack_endpoint` sur `true` dans un profil de votre AWS Config fichier pour diriger toutes les demandes Amazon S3 effectuées par les `s3api` AWS CLI commandes `s3` and vers le point de terminaison à double pile pour la région spécifiée. Vous spécifiez la région dans le fichier de configuration ou dans une commande à l'aide de l'option `--region`.

Lorsque vous utilisez des points de terminaison à double pile avec le style d'adressage AWS CLI, seul le style d'pathadressage est pris en charge. Le type d'adressage, défini dans le fichier de configuration, détermine si le nom du compartiment figure dans le nom d'hôte ou dans l'URL. Pour plus d'informations, consultez [s3outposts](#) dans le Guide de l'utilisateur AWS CLI .

Pour utiliser un point de terminaison à double pile via le AWS CLI, utilisez le `--endpoint-url` paramètre avec le point de terminaison `https://s3-outposts-fips.region.api.aws` terminaison `http://s3.dualstack.region.amazonaws.com` ou pour toute `s3outposts` commande `s3control` or.

Par exemple :

```
$ aws s3control list-regional-buckets --endpoint-url https://s3-outposts.region.api.aws
```

Utilisation de S3 sur les points de terminaison à double pile d'Outposts à partir du AWS SDKs

Cette section fournit des exemples de la manière d'accéder à un point de terminaison à double pile à l'aide du AWS SDKs.

AWS SDK for Java 2.x exemple de point de terminaison à double pile

Les exemples suivants montrent comment utiliser les classes `S3ControlClient` et `S3OutpostsClient` pour activer les points de terminaison à double pile lors de la création d'un client S3 sur Outposts à l'aide du kit AWS SDK for Java 2.x. Pour obtenir des instructions pour la création et le test d'un exemple pratique Java pour Amazon S3 sur Outposts, consultez [Commencer à utiliser le SDK AWS CLI and pour Java](#).

Exemple– Création d'une classe `S3ControlClient` avec les points de terminaison à double pile activés

```
import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3control.S3ControlClient;
import software.amazon.awssdk.services.s3control.model.ListRegionalBucketsRequest;
import software.amazon.awssdk.services.s3control.model.ListRegionalBucketsResponse;
import software.amazon.awssdk.services.s3control.model.S3ControlException;

public class DualStackEndpointsExample1 {

    public static void main(String[] args) {
        Region clientRegion = Region.of("us-east-1");
        String accountId = "111122223333";
        String navyId = "9876543210";

        try {
            // Create an S3ControlClient with dual-stack endpoints enabled.
            S3ControlClient s3ControlClient = S3ControlClient.builder()
                .region(clientRegion)
                .dualstackEnabled(true)
                .build();

            ListRegionalBucketsRequest listRegionalBucketsRequest =
                ListRegionalBucketsRequest.builder()
                    .accountId(accountId)
```

```

        .outpostId(navyId)

        .build();

        ListRegionalBucketsResponse listBuckets =
s3ControlClient.listRegionalBuckets(listRegionalBucketsRequest);
        System.out.printf("ListRegionalBuckets Response: %s%n",
listBuckets.toString());
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 on Outposts
couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    }
    catch (S3ControlException e) {
        // Unknown exceptions will be thrown as an instance of this type.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 on Outposts couldn't be contacted for a response, or the
client
        // couldn't parse the response from Amazon S3 on Outposts.
        e.printStackTrace();
    }
}
}
}

```

Example– Création d'un S3OutpostsClient avec les points de terminaison à double pile activés

```

import com.amazonaws.AmazonServiceException;
import com.amazonaws.SdkClientException;
import software.amazon.awssdk.regions.Region;
import software.amazon.awssdk.services.s3outposts.S3OutpostsClient;
import software.amazon.awssdk.services.s3outposts.model.ListEndpointsRequest;
import software.amazon.awssdk.services.s3outposts.model.ListEndpointsResponse;
import software.amazon.awssdk.services.s3outposts.model.S3OutpostsException;

public class DualStackEndpointsExample2 {

    public static void main(String[] args) {
        Region clientRegion = Region.of("us-east-1");

```

```
try {
    // Create an S3OutpostsClient with dual-stack endpoints enabled.
    S3OutpostsClient s3OutpostsClient = S3OutpostsClient.builder()
                                                .region(clientRegion)
                                                .dualstackEnabled(true)
                                                .build();

    ListEndpointsRequest listEndpointsRequest =
ListEndpointsRequest.builder().build();

    ListEndpointsResponse listEndpoints =
s3OutpostsClient.listEndpoints(listEndpointsRequest);
    System.out.printf("ListEndpoints Response: %s%n",
listEndpoints.toString());
    } catch (AmazonServiceException e) {
        // The call was transmitted successfully, but Amazon S3 on Outposts
couldn't process
        // it, so it returned an error response.
        e.printStackTrace();
    }
    catch (S3OutpostsException e) {
        // Unknown exceptions will be thrown as an instance of this type.
        e.printStackTrace();
    } catch (SdkClientException e) {
        // Amazon S3 on Outposts couldn't be contacted for a response, or the
client
        // couldn't parse the response from Amazon S3 on Outposts.
        e.printStackTrace();
    }
}
}
```

Si vous utilisez AWS SDK for Java 2.x le sous Windows, vous devrez peut-être définir la propriété de machine virtuelle Java (JVM) suivante :

```
java.net.preferIPv6Addresses=true
```

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.