

---

# Amazon Simple Storage Service

## Console User Guide



# Amazon Simple Storage Service: Console User Guide

Copyright © 2020 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

## Table of Contents

Bienvenue dans le guide de l'utilisateur de la console Amazon S3 .....	1
Modification de la langue de la console .....	2
Création et configuration d'un compartiment .....	3
Créer un compartiment .....	4
Plus d'informations .....	5
Suppression d'un compartiment .....	5
Plus d'informations .....	6
Vider un compartiment .....	6
Affichage des propriétés d'un compartiment .....	7
Activation ou désactivation de la gestion des versions .....	8
Activation du chiffrement par défaut .....	9
Plus d'informations .....	12
Activation de la journalisation des accès au serveur .....	13
Activation de la Journalisation au niveau des objets .....	15
Plus d'informations .....	18
Configuration de l'hébergement du site web statique .....	18
Étape 1 : Configurer un compartiment Amazon S3 pour l'hébergement du site web statique .....	18
Étape 2 : Modifier les paramètres de blocage de l'accès public .....	20
Étape 3 : Ajouter une stratégie de compartiment .....	22
Étape 4 : Tester le point de terminaison de votre site web .....	23
Redirection des demandes de sites web .....	23
Paramètres avancés .....	24
Configuration de la destination des notifications d'événements .....	24
Activation et configuration des notifications d'événements .....	26
Activation de Transfer Acceleration .....	31
Points d'accès .....	33
Création d'un point d'accès .....	33
Gestion et utilisation des points d'accès Amazon S3 .....	34
Chargement, téléchargement et gestion d'objets .....	36
Chargement d'objets S3 .....	37
Chargement de fichiers et de dossiers par glisser-déposer .....	38
Chargement de fichiers en pointant et en cliquant .....	43
Plus d'informations .....	44
Copier un objet .....	45
Déplacement d'un objet .....	45
Téléchargement d'objets S3 .....	46
Voir aussi .....	49
Suppression d'objets .....	49
Plus d'informations .....	50
Restauration d'objets .....	50
Plus d'informations .....	50
Restauration d'objets S3 archivés .....	51
Options de récupération des archives .....	51
Restauration d'un objet S3 archivé .....	52
La mise à niveau est une restauration en cours .....	54
Vérification du statut de la restauration et de la date d'expiration de l'archive .....	55
Verrouillage d'objets Amazon S3 .....	56
Plus d'informations .....	58
Affichage de la présentation d'un objet .....	58
Plus d'informations .....	61
Affichage des versions d'un objet .....	61
Plus d'informations .....	62
Affichage des propriétés d'un objet .....	62
Ajout du chiffrement à un objet .....	64

Plus d'informations .....	67
Ajout de métadonnées à un objet .....	67
Ajout de métadonnées définies par le système .....	68
Ajout de métadonnées définies par l'utilisateur .....	70
Ajout de balises à un objet .....	73
Plus d'informations .....	75
Utilisation de dossiers .....	75
Création d'un dossier .....	76
Suppression de dossiers .....	78
Rendre les dossiers publics .....	80
Opérations par lot S3 .....	81
Création d'une tâche Opérations par lot S3 .....	81
Plus d'informations .....	82
Gestion des tâches Opérations par lot S3 .....	82
Plus d'informations .....	82
Gestion du stockage .....	83
Création d'une stratégie de cycle de vie .....	83
Création de règles de réplication .....	87
Ajout d'une règle de réplication lorsque le compartiment de destination est dans le même compte AWS .....	89
Ajout d'une règle de réplication lorsque le compartiment de destination est dans un compte AWS distinct .....	96
Plus d'informations .....	103
Gestion des règles de réplication .....	103
Plus d'informations .....	105
Configuration d'une analyse de classe de stockage .....	105
Configuration de l'inventaire Amazon S3 .....	109
Stratégie du compartiment de destination .....	112
Autoriser Amazon S3 à utiliser votre CMK AWS KMS pour le chiffrement .....	113
Création d'un filtre de métriques des demandes pour un compartiment .....	114
Création d'un filtre de métriques des demandes à l'aide de balises ou de préfixes d'objet .....	115
Suppression d'un filtre de métriques des demandes .....	116
Affichage des métriques de réplication .....	117
Définition d'autorisations .....	118
Blocage d'accès public .....	119
Statut d'accès .....	119
Plus d'informations .....	120
Modification des paramètres d'accès public d'un compartiment .....	120
Modification des paramètres d'accès public pour un compartiment S3 .....	121
Modification des paramètres d'accès public pour plusieurs compartiments S3 .....	121
Plus d'informations .....	122
Modification des paramètres d'accès public d'un compte .....	123
Plus d'informations .....	123
Définition des autorisations d'un objet .....	124
Plus d'informations .....	127
Définition des autorisations de compartiment ACL .....	127
Plus d'informations .....	130
Ajout d'une stratégie de compartiment .....	131
Plus d'informations .....	132
Ajout du partage de ressources inter-domaines avec le partage CORS .....	132
Plus d'informations .....	133
Définir Propriété de l'objet sur le propriétaire du compartiment préféré .....	134
Comment puis-je m'assurer que je suis propriétaire des nouveaux objets ? .....	134
Utiliser Access Analyzer for S3 .....	134
Quelles sont les informations fournies par Access Analyzer for S3 ? .....	135
Activation d'Access Analyzer for S3 .....	136
Blocage de tous les accès publics .....	136

Vérification et modification de l'accès à un compartiment .....	137
Archivage des résultats de compartiment .....	138
Activation d'un résultat de compartiment archivé .....	139
Affichage des détails de résultats .....	139
Téléchargement d'un rapport Access Analyzer for S3 .....	139
Historique du document .....	140
Mises à jour antérieures .....	141
Glossaire AWS .....	143

# Bienvenue dans le guide de l'utilisateur de la console Amazon S3

Bienvenue dans le manuel Amazon Simple Storage Service Guide de l'utilisateur de la console de la console Amazon Simple Storage Service (Amazon S3).

Amazon S3 offre une solution de stockage sans limites virtuelles sur Internet. Ce manuel explique comment créer des compartiments, des objets et des dossiers dans Amazon S3 par l'intermédiaire de l'AWS Management Console, une interface graphique utilisateur basée sur un navigateur, destinée à interagir avec les services AWS.

Pour des informations conceptuelles détaillées sur le fonctionnement d'Amazon S3, consultez [Qu'est-ce qu'Amazon S3 ?](#) dans le Amazon Simple Storage Service Manuel du développeur. Le manuel du développeur contient également des informations détaillées sur les fonctions Amazon S3, ainsi que des exemples de code pour la prise en charge de ces fonctions.

## Rubriques

- [Création et configuration d'un compartiment S3 \(p. 3\)](#)
- [Chargement, téléchargement et gestion d'objets \(p. 36\)](#)
- [Gestion du stockage \(p. 83\)](#)
- [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#)

# Comment puis-je modifier la langue de la AWS Management Console ?

Vous pouvez modifier la langue d'affichage de la AWS Management Console. Plusieurs langues sont prises en charge.

Pour modifier la langue de la console

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Faites défiler vers le bas jusqu'à ce que la barre s'affiche au bas de la fenêtre, puis choisissez la langue dans la partie gauche de la barre.



3. Choisissez la langue de votre choix à partir du menu. Cela modifiera la langue pour l'ensemble d'AWS Management Console.



# Création et configuration d'un compartiment S3

Pour charger vos données (photos, vidéos, documents, etc.) dans Amazon S3, vous devez d'abord créer un compartiment S3 dans l'une des régions AWS. Vous pouvez ensuite charger les objets de données dans le compartiment.

Chaque objet que vous stockez dans Amazon S3 réside dans un compartiment. Vous pouvez utiliser des compartiments pour regrouper des objets connexes, comme lorsque vous utilisez un répertoire pour regrouper des fichiers dans un système de fichiers.

Amazon S3 crée des compartiments dans la région AWS que vous spécifiez. Vous pouvez choisir n'importe quelle région AWS géographiquement proche, afin d'optimiser la latence, de réduire les coûts ou de répondre à des exigences réglementaires. Par exemple, si vous résidez en Europe, il peut être avantageux de créer des compartiments dans les régions Europe (Irlande) ou Europe (Francfort). Pour obtenir la liste des régions AWS Amazon S3, consultez [Régions et points de terminaison](#) dans le Référence générale d'Amazon Web Services.

Vous n'êtes pas facturé pour la création d'un compartiment. La création d'un compartiment ne vous sera pas facturée. Seuls le stockage des objets dans le compartiment et le transfert des objets hors du compartiment le sont. Pour plus d'informations sur la tarification, consultez [FAQ sur Amazon Simple Storage Service \(S3\)](#).

Les noms de compartiment Amazon S3 sont uniques à l'échelle mondiale, quelle que soit la région AWS dans laquelle vous créez le compartiment. Vous nommez votre compartiment au moment de sa création. Pour obtenir des directives sur l'attribution d'un nom pour le compartiment, consultez [Limites et restrictions applicables aux compartiments](#) dans le Amazon Simple Storage Service Manuel du développeur.

Les rubriques suivantes expliquent comment utiliser la console Amazon S3 pour créer, supprimer et gérer des compartiments.

## Rubriques

- [Comment créer un compartiment S3 ? \(p. 4\)](#)
- [Comment supprimer un compartiment S3 ? \(p. 5\)](#)
- [Comment puis-je vider un compartiment S3 ? \(p. 6\)](#)
- [Comment afficher les propriétés d'un compartiment S3 ? \(p. 7\)](#)
- [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#)
- [Comment activer le chiffrement par défaut pour un compartiment Amazon S3 ? \(p. 9\)](#)
- [Comment activer la journalisation des accès au serveur pour un compartiment S3 ? \(p. 13\)](#)
- [Comment activer la journalisation au niveau des objets pour un compartiment S3 avec des événements de données AWS CloudTrail ? \(p. 15\)](#)
- [Comment configurer un compartiment S3 pour l'hébergement du site web statique ? \(p. 18\)](#)
- [Comment rediriger toutes les demandes à un site web hébergé dans un compartiment S3 vers un autre hôte ? \(p. 23\)](#)
- [Paramètres avancés pour les propriétés de compartiment S3 \(p. 24\)](#)



## Comment créer un compartiment S3 ?

Pour pouvoir charger des données dans Amazon S3, vous devez d'abord créer un compartiment dans l'une des régions AWS en vue de stocker vos données. Après avoir créé un compartiment, vous pouvez charger un nombre illimité d'objets de données dans ce compartiment.

Le compte AWS qui crée le compartiment en est le propriétaire. Par défaut, vous pouvez créer jusqu'à 100 compartiments par compte AWS. Si vous avez besoin de compartiments supplémentaires, vous pouvez augmenter votre quota de compartiments de compte à un maximum de 1 000 compartiments en soumettant une demande d'augmentation de quota de service. Pour en savoir plus sur l'augmentation de votre quota de compartiments, veuillez consulter [Quotas de service AWS](#) dans les Références générales AWS.

Les compartiments sont associés à des propriétés de configuration, dont leur région géographique, les paramètres d'accès aux objets qu'ils contiennent, ainsi que d'autres métadonnées.

Pour créer un compartiment

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez Créer un compartiment.
3. Dans Bucket name (Nom du compartiment), saisissez un nom compatible DNS pour votre compartiment.

Les caractéristiques du nom du compartiment doivent être les suivantes :

- Il doit être unique pour l'ensemble des compartiments Amazon S3.
- Il doit comporter entre 3 et 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 obtenir des informations sur la façon de nommer les compartiments, veuillez consulter [Règles relatives à l'attribution des noms de compartiments](#) dans le Amazon Simple Storage Service Manuel du développeur.

### 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.

4. Dans Region (Région), choisissez la région AWS dans laquelle le compartiment doit résider.

Choisissez une région proche de vous afin de limiter la latence et les coûts, et répondre aux exigences légales. Les objets stockés dans une région ne la quittent jamais, sauf si vous les transférez explicitement vers une autre région. Pour obtenir la liste des régions AWS Amazon S3, consultez les [Points de terminaison du service AWS](#) dans le Référence générale d'Amazon Web Services.

5. Dans Bucket settings for Block Public Acces (Paramètres de compartiment pour Bloquer l'accès public), choisissez les paramètres de blocage de l'accès public que vous souhaitez appliquer au compartiment.

Nous vous recommandons de laisser tous les paramètres activés, sauf si vous savez que vous devez en désactiver un ou plusieurs d'entre eux pour votre cas d'utilisation, par exemple pour héberger un site web public. Les paramètres de blocage de l'accès public que vous activez pour le compartiment seront également activés pour tous les points d'accès que vous créez dans le compartiment. Pour plus d'informations sur le blocage de l'accès public, consultez [Using Amazon S3 Block Public Access](#)

([Utilisation d'Amazon S3 Block Public Access](#)) dans le Amazon Simple Storage Service Manuel du développeur.

6. (Facultatif) Si vous souhaitez activer S3 Verrouillage d'objet :
  - a. Choisissez Advanced settings (Paramètres avancés) et lisez le message qui s'affiche.

#### Important

Vous ne pouvez activer S3 Verrouillage d'objet pour un compartiment que lorsque vous le créez. Si vous activez le Verrouillage d'objet pour le compartiment, vous ne pouvez pas le désactiver ultérieurement. L'activation de Verrouillage d'objet active également la gestion des versions pour le compartiment. Après avoir activé Verrouillage d'objet pour le compartiment, vous devez configurer les paramètres de Verrouillage d'objet avant que ceux du compartiment soient protégés. Pour plus d'informations sur la configuration de la protection des objets, consultez [Comment verrouiller un objet Amazon S3 ? \(p. 56\)](#).

- b. Si vous souhaitez activer le Verrouillage d'objet, saisissez activer dans la zone de texte et choisissez Confirmer.

Pour de plus amples informations sur la fonction S3 Verrouillage d'objet, veuillez consulter [Verrouillage d'objets à l'aide du verrou d'objets Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

7. Choisissez Créer un compartiment.

## Plus d'informations

- [Comment supprimer un compartiment S3 ? \(p. 5\)](#)
- [Comment définir des autorisations de compartiment ACL ? \(p. 127\)](#)

## Comment supprimer un compartiment S3 ?

Vous pouvez supprimer un compartiment vide et, lorsque vous utilisez AWS Management Console, vous pouvez supprimer un compartiment qui contient des objets. Si vous supprimez un compartiment qui contient des objets, tous les objets du compartiment sont définitivement supprimés.

Lorsque vous supprimez un compartiment activé pour la gestion des versions, toutes les versions de tous les objets du compartiment sont définitivement supprimées. Pour plus d'informations sur la gestion des versions, consultez [Gestion des objets dans un compartiment activé pour la gestion des versions](#) dans le Amazon Simple Storage Service Manuel du développeur.

Avant de supprimer un compartiment, tenez compte des points suivants :

- Les noms de compartiment sont uniques. Si vous supprimez un compartiment, un autre utilisateur AWS peut en utiliser le nom.
- Si vous supprimez un compartiment qui contient des objets, tous ces objets sont définitivement supprimés, y compris ceux qui ont été transmis à la classe de stockage S3 Glacier.
- Si le compartiment héberge un site web statique, et que vous avez créé et configuré une zone hébergée Amazon Route 53 comme décrit dans [Créer et configurer une zone hébergée Amazon Route 53](#), vous devez effacer les paramètres de la zone hébergée Route 53 qui sont associés au compartiment comme décrit dans [Supprimer la zone hébergée Route 53](#).
- Si le compartiment reçoit les données de journaux depuis Elastic Load Balancing (ELB), il est recommandé de cesser la remise des journaux ELB au compartiment avant de le supprimer. Après que vous avez supprimé le compartiment, si un autre utilisateur crée un compartiment à l'aide du même

nom, vos données de journaux peuvent potentiellement être remises à ce compartiment. Pour plus d'informations sur les journaux d'accès ELB, consultez [Journaux d'accès](#) dans le Guide de l'utilisateur pour les Equilibreurs de charge classiques et [Journaux d'accès](#) dans le Guide de l'utilisateur pour les Application Load Balancers.

### Important

Si vous souhaitez réutiliser le même nom de compartiment, ne supprimez pas le compartiment. Nous vous recommandons de vider le compartiment et de le conserver. Une fois un compartiment supprimé, son nom peut être réutilisé. Cependant, il est possible que cela ne soit pas possible pour différentes raisons. Par exemple, il peut s'écouler un certain temps avant que le nom ne puisse être réutilisé et un autre compte peut créer un compartiment portant ce nom avant vous.

### Pour supprimer un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste des Buckets (Compartiments), sélectionnez l'option en regard du nom du compartiment à supprimer, puis choisissez Delete (Supprimer) en haut de la page.
3. Dans la page Delete bucket (Supprimer le compartiment), confirmez que vous souhaitez supprimer le compartiment en saisissant le nom de ce dernier dans le champ de texte, puis choisissez Delete bucket (Supprimer le compartiment).

### Note

Si le compartiment contient des objets, videz-le avant de le supprimer en sélectionnant le lien de configuration du compartiment vide dans l'alerte d'erreur This bucket is not empty (Ce compartiment n'est pas vide) et en suivant les instructions de la page Empty bucket (Compartiment vide). Revenez ensuite à la page Delete bucket (Supprimer le compartiment) et supprimez le compartiment.

## Plus d'informations

- [Comment puis-je vider un compartiment S3 ? \(p. 6\)](#)
- [Comment supprimer des objets d'un compartiment S3 ? \(p. 49\)](#)

## Comment puis-je vider un compartiment S3 ?

Vous pouvez vider un compartiment, ce qui entraîne la suppression de tous les objets du compartiment, sans supprimer ce dernier. Lorsque vous videz un compartiment activé pour la gestion des versions, toutes les versions de tous les objets du compartiment sont supprimées. Pour plus d'informations, consultez [Gestion des objets dans un compartiment activé pour le contrôle de version](#) et [Suppression ou vidage d'un compartiment](#) dans le Amazon Simple Storage Service Manuel du développeur.

### Pour vider un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Bucket name (Nom du compartiment), sélectionnez l'option en regard du nom du compartiment à vider, puis choisissez Empty (Vider).
3. Sur la page Empty bucket (Vider le compartiment), confirmez que vous souhaitez vider le compartiment en saisissant le nom de ce dernier dans le champ de texte, puis choisissez Empty (Vider).

4. (Facultatif) Surveillez la progression du processus de vidage du compartiment sur la page Empty bucket status (Statut du compartiment vide).

### Warning

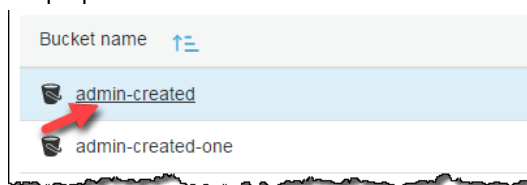
Cette action supprime tous les objets du compartiment. Attendez la fin du vidage du compartiment se termine avant d'ajouter de nouveaux objets. Les nouveaux objets peuvent être supprimés s'ils sont ajoutés pendant que le processus de vidage compartiment est en cours.

## Comment afficher les propriétés d'un compartiment S3 ?

Cette rubrique explique comment afficher les propriétés d'un compartiment S3.

Pour afficher les propriétés d'un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, sélectionnez le nom du compartiment dont vous souhaitez afficher les propriétés.



3. Choisissez Properties.



4. Sur la page Propriétés, vous pouvez configurer les propriétés suivantes pour le compartiment.
  - a. Gestion des versions – La gestion des versions vous permet de conserver plusieurs versions d'un objet au sein d'un même compartiment. Par défaut, la gestion des versions est désactivée pour un nouveau compartiment. Pour plus d'informations sur l'activation de la gestion des versions, consultez [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#).
  - b. Journalisation des accès au serveur – La journalisation des accès au serveur fournit des enregistrements détaillés sur les demandes portant sur votre compartiment. Par défaut, Amazon S3 ne collecte pas les journaux d'accès au serveur. Pour plus d'informations sur l'activation de la journalisation des accès au serveur, consultez [Comment activer la journalisation des accès au serveur pour un compartiment S3 ? \(p. 13\)](#).
  - c. Hébergement de site web statique – Vous pouvez héberger un site web statique sur Amazon S3. Pour activer cette option, choisissez Hébergement de site Web statique, puis spécifiez les paramètres que vous voulez utiliser. Pour plus d'informations, consultez [Comment configurer un compartiment S3 pour l'hébergement du site web statique ? \(p. 18\)](#).
  - d. Journalisation au niveau des objets – La journalisation au niveau des objets enregistre l'activité de l'API au niveau des objets à l'aide d'événements de données CloudTrail. Pour plus d'informations sur l'activation de la journalisation au niveau des objets, consultez [Comment activer](#)

la journalisation au niveau des objets pour un compartiment S3 avec des événements de données AWS CloudTrail ? (p. 15).

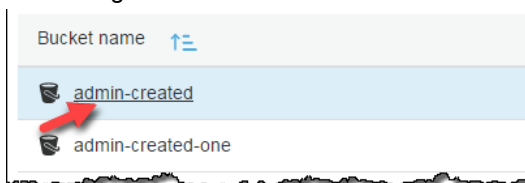
- e. Balises – Grâce à la répartition des coûts AWS, vous pouvez utiliser des balises de compartiment pour annoter la facturation relative à l'utilisation d'un compartiment. Une balise correspond à une paire clé-valeur représentant un libellé que vous affectez à un compartiment. Pour ajouter des balises, cliquez sur Balises, puis sur Ajouter une balise. Pour plus d'informations, consultez [Utilisation des balises de répartition des coûts pour les compartiments S3](#) dans le Amazon Simple Storage Service Manuel du développeur.
- f. Transfer Acceleration – Amazon S3 Transfer Acceleration permet un transfert rapide, facile et sécurisé des fichiers sur de longues distances entre votre client et un compartiment S3. Pour plus d'informations sur l'activation de l'accélération du transfert, consultez [Comment activer Transfer Acceleration pour un compartiment S3 ?](#) (p. 31).
- g. Événements – Vous pouvez autoriser certains événements de compartiment Amazon S3 à envoyer un message de notification à une destination chaque fois que certains événements se produisent. Pour activer cette option, choisissez Événements, puis spécifiez les paramètres que vous voulez utiliser. Pour plus d'informations, consultez [Comment activer et configurer des notifications d'événements pour un compartiment S3 ?](#) (p. 26).
- h. Paiement par le demandeur – Vous pouvez activer le paiement par le demandeur pour que le demandeur (plutôt que le propriétaire du compartiment) règle les demandes et les transferts de données. Pour plus d'informations, consultez [Compartiments de type Paiement par le demandeur](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Comment activer ou interrompre la gestion des versions d'un compartiment S3 ?

La gestion des versions vous permet de conserver plusieurs versions d'un objet au sein d'un même compartiment. Cette section explique comment activer la gestion des versions d'objets dans un compartiment. Pour plus d'informations sur la prise en charge de la gestion des versions dans Amazon S3, consultez [Gestion des versions d'un objet](#) et [Utilisation de la gestion des versions](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour activer ou désactiver la gestion des versions dans un compartiment S3

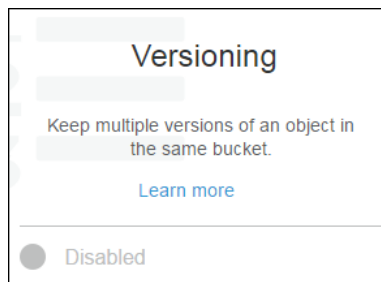
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez activer la gestion des versions.



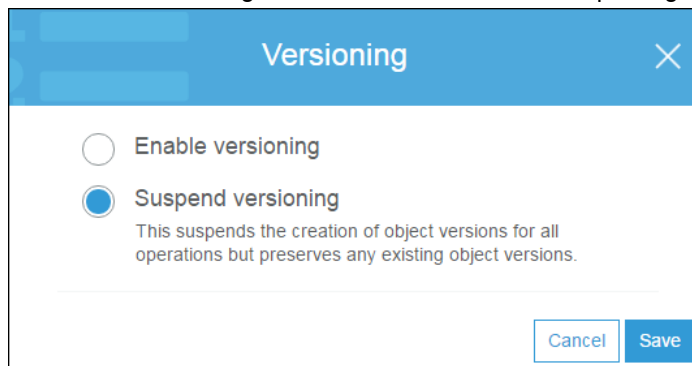
3. Choisissez Properties.



4. Choisissez Contrôle de version.



5. Choisissez Activer la gestion des versions ou Interrompre la gestion des versions, puis Enregistrer.



#### Note

Vous pouvez utiliser l'authentification multi-facteurs (MFA) AWS avec la gestion des versions. Lorsque vous utilisez l'authentification multi-facteurs (MFA) avec la gestion des versions, vous devez fournir les clés d'accès de votre compte AWS et un code valide à partir du périphérique MFA du compte afin de supprimer définitivement la version d'un objet ou de suspendre ou réactiver la gestion des versions. Pour utiliser l'authentification multi-facteurs (MFA) avec la gestion des versions, vous activez `MFA Delete`. Toutefois, vous ne pouvez pas activer `MFA Delete` à l'aide d'AWS Management Console. Vous devez utiliser l'interface de ligne de commande ou l'API AWS. Pour de plus amples informations, veuillez consulter [Fonction Supprimer MFA](#).

## Comment activer le chiffrement par défaut pour un compartiment Amazon S3 ?

Le chiffrement par défaut Amazon S3 fournit un moyen de définir le comportement de chiffrement par défaut pour un compartiment Amazon S3. Vous pouvez définir le chiffrement par défaut sur un compartiment afin que tous les objets soient chiffrés lorsqu'ils sont stockés dans le compartiment. Les objets sont chiffrés au moyen du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) ou par les clés CMK AWS Key Management Service (AWS KMS).

Lorsque vous utilisez le chiffrement côté serveur, Amazon S3 chiffre un objet avant de l'enregistrer sur disque dans ses centres de données et le déchiffre lorsque vous téléchargez l'objet. Pour plus d'informations sur la protection des données à l'aide du chiffrement côté serveur et de la gestion de clés de chiffrement, consultez [Protection des données à l'aide du chiffrement côté serveur](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

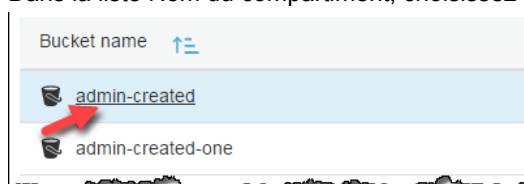
Le chiffrement par défaut fonctionne avec tous les compartiments Amazon S3 nouveaux et existants. Sans le chiffrement par défaut, pour chiffrer tous les objets stockés dans un compartiment, vous devez

inclure les informations de chiffrement dans chaque demande de stockage d'objets. Vous devez également configurer une stratégie de compartiment Amazon S3 de manière à rejeter les demandes de stockage qui ne comportent pas d'informations de chiffrement.

Il n'y a pas de frais supplémentaires relatifs à l'utilisation du chiffrement par défaut pour les compartiments S3. Les demandes de configuration de la fonction de chiffrement par défaut seront facturées comme les demandes Amazon S3 standard. Pour plus d'informations sur la tarification, consultez [Tarification Amazon S3](#). Pour le stockage des clés CMK SSE-KMS, des frais AWS KMS s'appliquent et sont répertoriés sous [Tarification AWS KMS](#).

Pour activer le chiffrement par défaut pour un compartiment Amazon S3

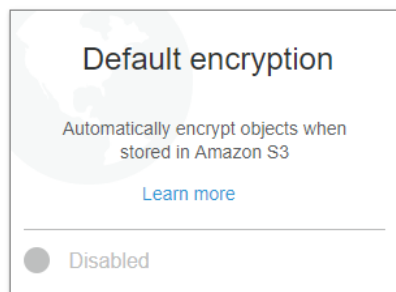
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.



3. Choisissez Propriétés.



4. Choisissez Chiffrement par défaut.



5. Si vous souhaitez utiliser des clés gérées par Amazon S3 pour le chiffrement par défaut, choisissez AES-256 et sélectionnez Enregistrer.

Pour plus d'informations sur l'utilisation du chiffrement côté serveur d'Amazon S3, consultez [Protection des données avec des clés de chiffrement gérées par Amazon S3](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Default encryption

This property does not affect existing objects in your bucket.

☐ None

☒ AES-256  
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

☐ AWS-KMS  
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Amazon S3 evaluates and applies bucket policies before applying bucket encryption settings. Even if you enable bucket encryption settings, your PUT requests without encryption information will be rejected if you have bucket policies to reject such PUT requests. Check your bucket policy and modify it if required.

[View bucket policy](#)

[Cancel](#) [Save](#)

### Important

Vous devrez peut-être mettre à jour votre stratégie de compartiment lors de l'activation du chiffrement par défaut. Pour plus d'informations, consultez [Passage au chiffrement par défaut à partir de stratégies de compartiments pour l'application du chiffrement](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

6. Si vous souhaitez utiliser les clés CMK stockées dans AWS KMS pour le chiffrement par défaut, procédez comme suit :
  - a. Choisissez AWS-KMS.
  - b. Pour sélectionner une clé CMK AWS KMS gérée par le client que vous avez créée, utilisez l'une des méthodes suivantes :
    - Dans la liste qui s'affiche, choisissez la clé CMK AWS KMS.
    - Dans la liste qui s'affiche, choisissez Custom KMS ARN (ARN KMS personnalisé), puis entrez l'ARN (Amazon Resource Name) de la clé CMK AWS KMS.

### Important

Vous pouvez utiliser uniquement les clés CMK KMS activées dans la même région AWS que le compartiment. La console S3 ne répertorie que 100 clés CMK KMS par région. Si vous avez plus de 100 clés CMK dans la même région, vous ne pouvez voir que les 100 premières clés CMK dans la console S3. Pour utiliser une clé CMK KMS qui n'est pas répertoriée dans la console, choisissez ARN KMS personnalisé, puis saisissez l'ARN CMK KMS.

Lorsque vous utilisez une clé CMK AWS KMS pour le chiffrement côté serveur dans Amazon S3, vous devez choisir une clé CMK symétrique. Amazon S3 ne prend en charge que les clés CMK symétriques et les clés CMK non asymétriques. Pour de plus amples informations, veuillez consulter [Utilisation des clés symétriques et asymétriques](#) dans le Manuel du développeur AWS Key Management Service.



**Default encryption** [X]

This property does not affect existing objects in your bucket.

☐ None

☐ AES-256  
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

☒ AWS-KMS  
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Custom KMS ARN [v]

Type to search [Q]

aws/s3

ca-key

Custom KMS ARN

View bucket policy

Cancel Save

### Important

Si vous utilisez l'option AWS KMS pour votre configuration de chiffrement par défaut, vous êtes soumis aux limites RPS (requêtes par seconde) d'AWS KMS. Pour plus d'informations sur les limites d'AWS KMS et sur la manière de demander une augmentation de limite, consultez [Limites d'AWS KMS](#).

Pour plus d'informations sur la création d'une clé CMK AWS KMS, consultez [Création de clés](#) dans le AWS Key Management Service Developer Guide. Pour plus d'informations sur la façon d'utiliser AWS KMS avec Amazon S3, consultez [Protection des données avec des clés stockées dans AWS KMS](#) dans le Amazon Simple Storage Service Manuel du développeur.

7. Choisissez Save.

## Plus d'informations

- [Chiffrement par défaut d'Amazon S3 pour compartiments S3](#) dans le manuel Amazon Simple Storage Service Manuel du développeur
- [Comment ajouter le chiffrement à un objet S3 ? \(p. 64\)](#)

## Comment activer la journalisation des accès au serveur pour un compartiment S3 ?

Cette rubrique explique comment activer la journalisation des accès au serveur pour un compartiment Amazon S3 à l'aide d'AWS Management Console. Pour plus d'informations sur l'activation de la journalisation par programmation et des détails sur la façon dont les journaux sont livrés, consultez [Journalisation des accès au serveur](#) dans le Amazon Simple Storage Service Manuel du développeur.

Par défaut, Amazon Simple Storage Service (Amazon S3) ne collecte pas les journaux d'accès au serveur. Lorsque vous activez la journalisation, Amazon S3 fournit des journaux d'accès pour un compartiment source dans un compartiment cible de votre choix. Le compartiment cible doit être situé dans la même région AWS que le compartiment source et ne doit pas présenter de configuration par défaut pour la période de rétention.

La journalisation des accès au serveur fournit des enregistrements détaillés pour les demandes soumises à un compartiment S3. Les journaux d'accès au serveur sont utiles pour de nombreuses applications. Par exemple, les informations des journaux d'accès peuvent s'avérer utiles en cas d'audit de sécurité ou d'audit des accès. Elles peuvent également vous permettre d'en savoir plus sur votre clientèle et de comprendre votre facture Amazon S3.

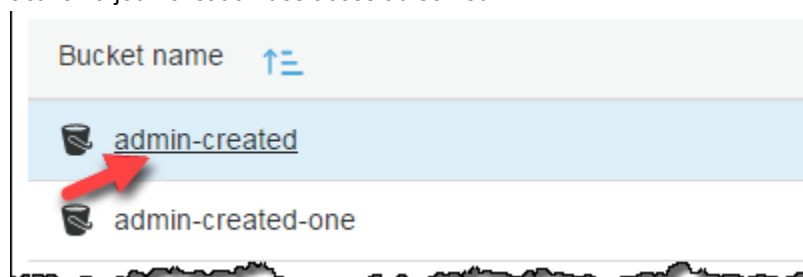
Un enregistrement de journal d'accès contient des détails relatifs aux demandes soumises à un compartiment. Ces informations peuvent comprendre le type de demande, les ressources spécifiées dans la demande, ainsi que l'heure et la date du traitement de la demande. Pour plus d'informations, consultez [Format des journaux d'accès au serveur](#) dans le Amazon Simple Storage Service Manuel du développeur.

### Important

L'activation de la journalisation des accès au serveur sur un compartiment Amazon S3 n'entraîne aucuns frais supplémentaires. Toutefois, les fichiers journaux qui vous sont fournis par le système augmentent les coûts de stockage habituels. Notez que vous pouvez supprimer les fichiers journaux à tout moment. Nous n'évaluons pas les frais de transfert de données pour l'envoi des fichiers journaux, mais nous facturons des frais standards de transfert de données pour l'accès aux fichiers journaux.

Pour activer la journalisation des accès au serveur pour un compartiment S3

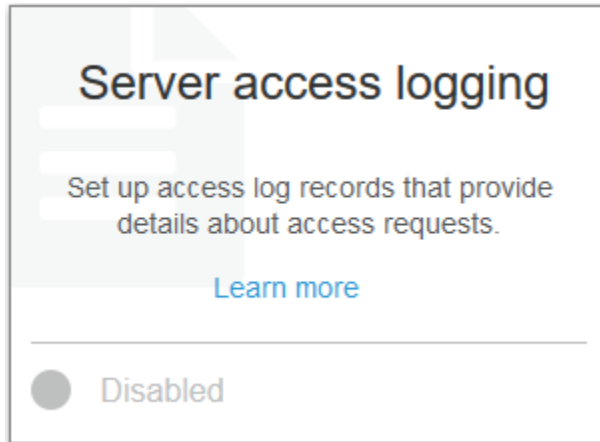
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez activer la journalisation des accès au serveur.



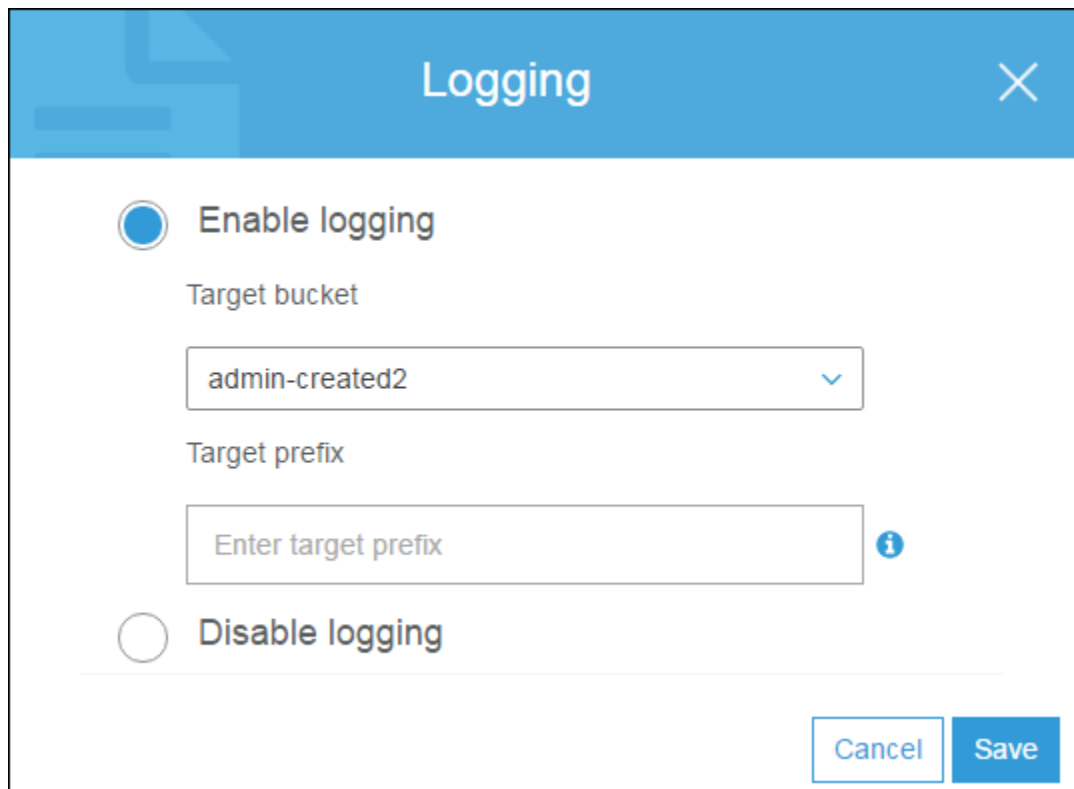
3. Choisissez Properties (Propriétés).



4. Choisissez Server access logging.



5. Choisissez Activer la journalisation. Pour Target (Cible), choisissez le nom du compartiment qui recevra les objets des enregistrements de journal. Le compartiment cible doit être situé dans la même région que le compartiment source et ne doit pas présenter de configuration par défaut pour la période de rétention.



6. (Facultatif) Pour Préfixe cible, saisissez un préfixe de nom de clé pour des objets de journaux, de sorte que tous les noms d'objet de journal commencent par la même chaîne.

7. Choisissez Save.

Vous pouvez afficher les journaux dans le compartiment cible. Si vous avez spécifié un préfixe, le préfixe s'affiche en tant que dossier dans le compartiment cible dans la console. Une fois que vous avez activé la journalisation des accès au serveur, cela peut prendre quelques heures avant que les journaux sont livrés dans le compartiment cible. Pour plus d'informations sur comment et quand les journaux sont livrés, consultez [Journalisation des accès au serveur](#) dans le Amazon Simple Storage Service Manuel du développeur.

Plus d'informations

[Comment afficher les propriétés d'un compartiment S3 ? \(p. 7\)](#)

## Comment activer la journalisation au niveau des objets pour un compartiment S3 avec des événements de données AWS CloudTrail ?

Cette section explique comment activer un journal de suivi AWS CloudTrail afin de journaliser des événements de données pour des objets dans un compartiment S3 à l'aide de la console Amazon S3. CloudTrail prend en charge la journalisation des opérations API au niveau de l'objet Amazon S3 telles que `GetObject`, `DeleteObject` et `PutObject`. Ces événements sont appelés événements de données. Par défaut, les journaux de suivi CloudTrail ne journalisent pas les événements de données, mais vous pouvez les configurer pour consigner les événements de données pour des compartiments S3 que vous spécifiez ou pour consigner les événements de données de tous les compartiments Amazon S3 de votre compte AWS. Pour plus d'informations, consultez [Journalisation des appels d'API Amazon S3 à l'aide AWS CloudTrail](#). CloudTrail ne remplit pas les événements de données dans l'historique des événements CloudTrail. En outre, toutes les actions au niveau du compartiment ne sont pas renseignées dans l'historique des événements CloudTrail. Pour plus d'informations, consultez [Utilisation de modèles de filtre Amazon CloudWatch Logs et Amazon Athena pour interroger les journaux CloudTrail](#).

Pour configurer un journal de suivi afin de consigner les événements de données pour un compartiment S3, vous pouvez utiliser la console AWS CloudTrail ou la console Amazon S3. Si vous configurez un journal de suivi afin de consigner les événements de données pour tous les compartiments Amazon S3 de votre compte AWS, il est plus facile d'utiliser la console CloudTrail. Pour plus d'informations sur l'utilisation de la console CloudTrail pour configurer un journal de suivi afin de consigner les événements de données S3, consultez [Événements de données](#) dans le AWS CloudTrail User Guide.

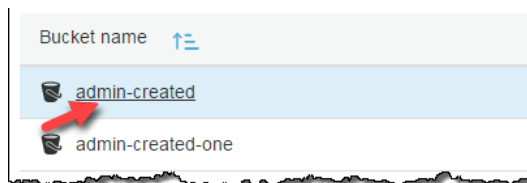
### Important

Des frais supplémentaires sont facturés pour les événements de données. Pour en savoir plus, consultez [Tarification AWS CloudTrail](#).

La procédure suivante montre comment utiliser la console Amazon S3 pour activer un journal de suivi CloudTrail afin de consigner les événements de données pour un compartiment S3.

Pour activer la journalisation des événements de données CloudTrail pour des objets d'un compartiment S3.

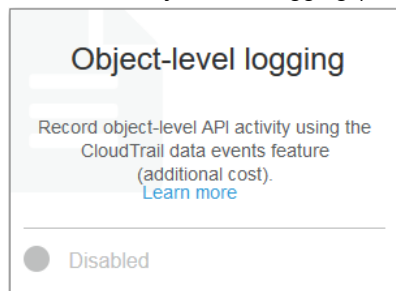
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.



3. Choisissez Propriétés.



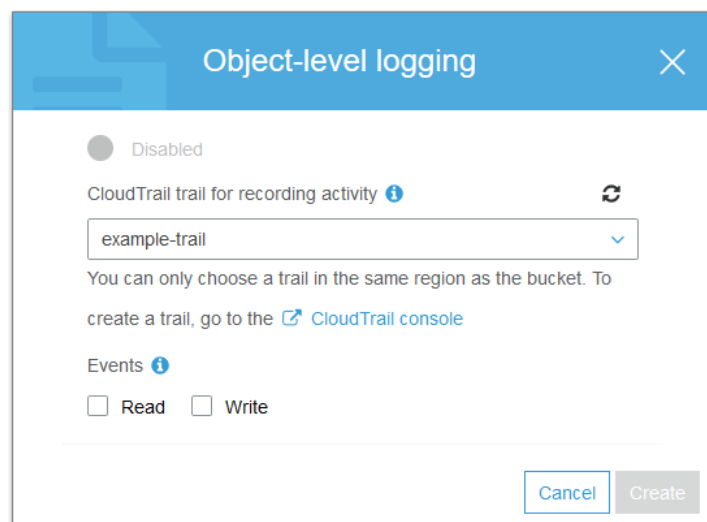
4. Choisissez Object-level logging (Journalisation au niveau des objets).



5. Choisissez un journal de suivi CloudTrail existant dans le menu déroulant.

Le journal de suivi que vous sélectionnez doit être situé dans la même région AWS que votre compartiment. La liste déroulante ne contient donc que les journaux de suivi qui se trouvent dans la même région que le compartiment ou les journaux de suivi qui ont été créés pour toutes les régions.

Si vous avez besoin d'en créer un, choisissez le lien de console CloudTrail pour accéder à la console CloudTrail. Pour plus d'informations sur la façon de créer des journaux de suivi dans la console CloudTrail, consultez [Création d'un journal de suivi avec la console](#) dans le AWS CloudTrail User Guide.

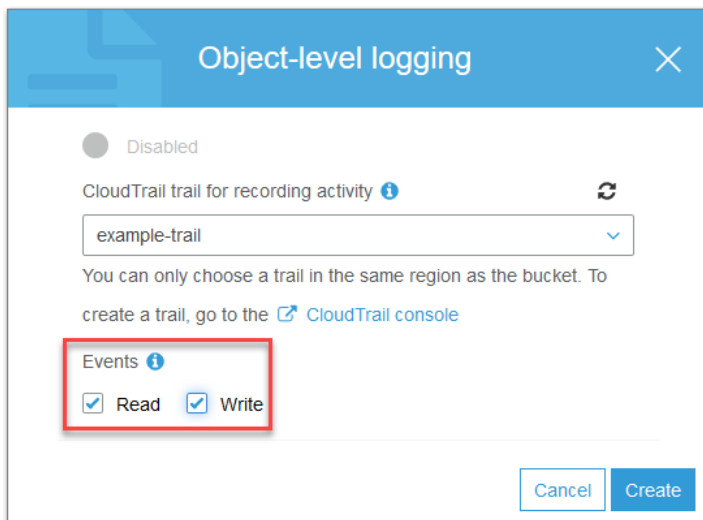


6. Sous Événements, choisissez l'une des options suivantes :

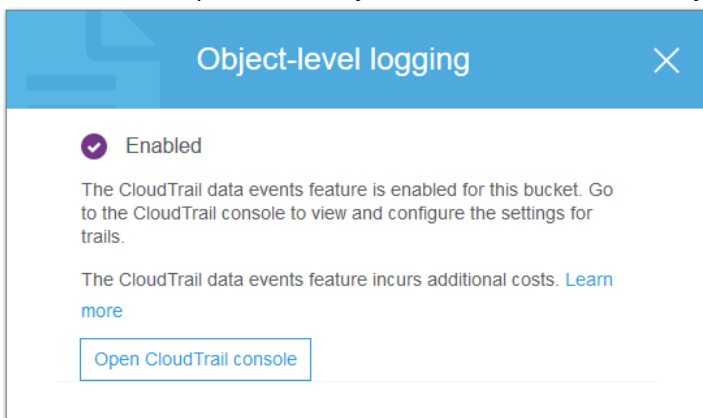
- Lire pour spécifier que vous souhaitez que CloudTrail consigne les API de lecture Amazon S3 telles que `GetObject`.
- Écrire pour consigner les API d'écriture Amazon S3 telles que `PutObject`.

- Lire et Écrire pour consigner les API de lecture et d'écriture d'objet.

Pour obtenir une liste des événements de données pris en charge journalisés par CloudTrail pour les objets Amazon S3, consultez [Actions au niveau de l'objet Amazon S3 suivies par la journalisation CloudTrail](#) dans le Amazon Simple Storage Service Manuel du développeur.



7. Choisissez Créer pour activer la journalisation au niveau des objets pour le compartiment.



Pour désactiver la journalisation au niveau des objets pour le compartiment, vous devez accéder à la console CloudTrail et supprimer le nom du compartiment de Data events (Événements de données) dans le journal de suivi.

#### Note

Si vous utilisez la console CloudTrail ou la console Amazon S3 pour configurer un journal de suivi afin de consigner les événements de données pour un compartiment S3, la console Amazon S3 indique que la journalisation au niveau des objets est activée pour le compartiment.

Pour plus d'informations sur l'activation de la journalisation au niveau des objets lorsque vous créez un compartiment S3, consultez [Comment créer un compartiment S3 ? \(p. 4\)](#).

## Plus d'informations

- [Comment afficher les propriétés d'un compartiment S3 ? \(p. 7\)](#)
- [Journalisation des appels d'API Amazon S3 à l'aide d'AWS CloudTrail](#) dans le Amazon Simple Storage Service Manuel du développeur
- [Utilisation de fichiers journaux CloudTrail](#) dans le AWS CloudTrail User Guide

## Comment configurer un compartiment S3 pour l'hébergement du site web statique ?

Vous pouvez héberger un site Web statique sur Amazon S3. Sur un site Web statique, les pages Web individuelles contiennent du contenu statique. Un site web statique peut également contenir des scripts côté client. Par contre, un site Web dynamique repose sur un traitement côté serveur, comprenant des scénarios côté serveur tels que PHP, JSP ou ASP.NET. Amazon S3 ne prend pas en charge l'écriture de scénario côté serveur.

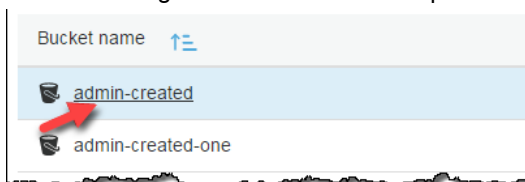
Vous pouvez utiliser les procédures rapides suivantes pour configurer un compartiment S3 pour l'hébergement de site web statique dans la console Amazon S3. Pour de plus amples informations, veuillez consulter [Hébergement d'un site Web statique sur Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur. Pour de plus amples informations sur la configuration d'un site Web statique avec un domaine personnalisé, veuillez consulter [Configuration d'un site web statique à l'aide d'un domaine personnalisé enregistré avec Route 53](#) dans le Amazon Simple Storage Service Manuel du développeur.

### Rubriques

- [Étape 1 : Configurer un compartiment Amazon S3 pour l'hébergement du site web statique \(p. 18\)](#)
- [Étape 2 : Modifier les paramètres de blocage de l'accès public \(p. 20\)](#)
- [Étape 3 : Ajouter une stratégie de compartiment \(p. 22\)](#)
- [Étape 4 : Tester le point de terminaison de votre site web \(p. 23\)](#)

## Étape 1 : Configurer un compartiment Amazon S3 pour l'hébergement du site web statique

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez activer l'hébergement de site web statique.



3. Choisissez Propriétés.



4. Choisissez Hébergement de site Web statique.



5. Choisissez Utiliser ce compartiment pour héberger un site Web.



6. Dans Document d'index, tapez le nom du document d'index, généralement `index.html`.

Lorsque vous configurez un compartiment pour l'hébergement d'un site Web, vous devez spécifier le document d'index, Amazon S3 renvoie ce document d'index lorsque des demandes sont faites au domaine racine ou à n'importe quel sous-répertoire. Pour de plus amples informations, veuillez consulter [Configuration de la prise en charge des documents d'index](#) dans le Amazon Simple Storage Service Manuel du développeur.

7. (Facultatif) Si vous souhaitez fournir votre propre document d'erreur personnalisé pour les erreurs de classe 4XX, entrez le nom du fichier du document d'erreur personnalisé dans Document d'erreur.

Si vous ne spécifiez pas de document d'erreur personnalisé et qu'une erreur se produit, Amazon S3 renvoie un document d'erreur HTML par défaut. Pour plus d'informations, consultez [Prise en charge de documents d'erreurs personnalisés](#) dans le Amazon Simple Storage Service Manuel du développeur.

8. (Facultatif) Si vous souhaitez spécifier des règles de redirection avancées, décrivez les règles à l'aide du langage XML dans Edit redirection rules (Modifier les règles de redirection).

Par exemple, vous pouvez acheminer les demandes de façon conditionnelle en fonction des noms ou préfixes de clés d'objets dans la demande. Pour de plus amples informations, veuillez consulter [Redirections conditionnelles avancées](#) dans le Amazon Simple Storage Service Manuel du développeur.



Static website hosting

Endpoint : <http://static-website-public.s3-website-us-west-2.amazonaws.com>

☒ Use this bucket to host a website [Learn more](#)

Index document [i](#)

Error document [i](#)

Redirection rules (optional) [i](#)

☐ Redirect requests [Learn more](#)

☐ Disable website hosting

☒ Disabled

9. Choisissez Enregistrer.
10. Chargez le document d'index dans votre compartiment.

Pour obtenir des instructions pas à pas sur le chargement d'un objet dans un compartiment S3, veuillez consulter [Chargement de fichiers en pointant et en cliquant \(p. 43\)](#).

11. Chargez d'autres fichiers pour votre site web, y compris les documents d'erreur personnalisés facultatifs.

Dans la section suivante, vous définissez les autorisations requises pour accéder à votre compartiment en tant que site web statique.

## Étape 2 : Modifier les paramètres de blocage de l'accès public

Par défaut, Amazon S3 bloque l'accès public à votre compte et à vos compartiments. Si vous souhaitez utiliser un compartiment pour héberger un site web statique, vous pouvez utiliser ces étapes pour modifier vos paramètres de blocage de l'accès public.

### Warning

Avant de terminer cette étape, revoyez [Utilisation du blocage de l'accès public Amazon S3](#) pour vous assurer que vous comprenez et acceptez les risques liés à l'autorisation d'accès public. Lorsque vous désactivez les paramètres de blocage d'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tout accès public à vos compartiments.

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez le nom du compartiment que vous avez configuré en tant que site web statique.
3. Choisissez Permissions.
4. Choisissez Modifier.
5. Effacez Block all public access (Bloquer tous les accès publics) et choisissez Save (Enregistrer).

#### Warning

Avant de terminer cette étape, revoyez [Utilisation du blocage de l'accès public Amazon S3](#) pour vous assurer que vous comprenez et acceptez les risques liés à l'autorisation d'accès public. Lorsque vous désactivez les paramètres de blocage d'accès public pour rendre votre compartiment public, toute personne sur Internet peut accéder à votre compartiment. Nous vous recommandons de bloquer tout accès public à vos compartiments.

## Edit block public access settings for selected buckets

Total buckets: 1 (Public: 0)

### Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to buckets and objects is blocked, turn on Block *all* public access. These settings apply only to selected buckets. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. [Learn more](#)

The Block public access settings turned on at the account level affect public access to all buckets in the account. To determine which settings are checked, check your Block public access (account settings).

☒ **Block *all* public access**

Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

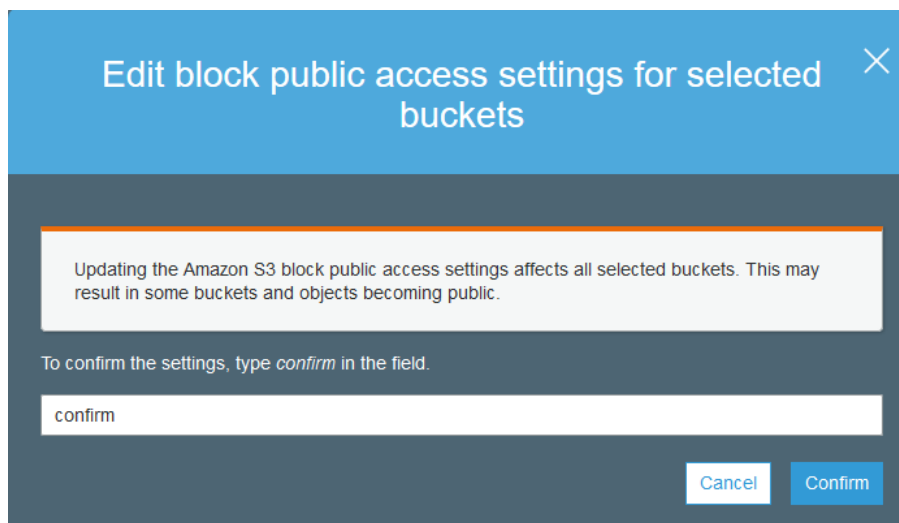
☒ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**

S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.

☒ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**

S3 will ignore all ACLs that grant public access to buckets and objects.

6. Dans la zone de confirmation, entrez **confirm**, puis choisissez Confirm (Confirmer).



Sous S3 buckets (Compartiments S3), l'Access (Accès) de votre compartiment devient Objects can be public (Les objets peuvent être publics). Vous pouvez désormais ajouter une stratégie de compartiment pour rendre les objets du compartiment lisibles publiquement. Si l'Access (Accès) continue de s'afficher comme Bucket and objects not public (Compartiment et objets non publics), vous devrez peut-être [modifier les paramètres de blocage de l'accès public](#) pour votre compte avant d'ajouter une stratégie de compartiment.

## Étape 3 : Ajouter une stratégie de compartiment

Après avoir modifié les paramètres de S3 Block Public Access, vous devez ajouter une stratégie de compartiment pour accorder un accès public en lecture à votre compartiment. Lorsque vous accordez un accès public en lecture, tout le monde sur Internet peut accéder à votre compartiment.

### Important

La stratégie suivante est uniquement un exemple et autorise un accès complet au contenu de votre compartiment. Avant de réaliser cette étape, consultez [Comment puis-je sécuriser les fichiers de mon compartiment Amazon S3 ?](#), pour vous assurer que vous comprenez les meilleures pratiques pour sécuriser les fichiers dans votre compartiment S3 et les risques liés à l'octroi d'un accès public.

1. Dans Buckets (Compartiments), choisissez le nom de votre compartiment.
2. Choisissez Permissions.
3. Choisissez Stratégie de compartiment.
4. Pour accorder l'accès public en lecture à votre site web, copiez la stratégie de compartiment suivante et collez-la dans l'Éditeur de stratégie de compartiment.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "PublicReadGetObject",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
```

```
    "arn:aws:s3:::example.com/*"  
  ]  
}  
]
```

5. Mettez à jour `Resource` pour inclure le nom de votre compartiment.

Dans l'exemple de stratégie de compartiment précédent, `example.com` est le nom de compartiment. Pour utiliser cette stratégie de compartiment avec votre propre compartiment, vous devez mettre à jour ce nom pour qu'il corresponde à celui de votre compartiment.

6. Choisissez Enregistrer.

Un avertissement s'affiche et indique que le compartiment a un accès public. Dans Bucket Policy (Stratégie de compartiment), une étiquette Public apparaît.

Si une erreur indique `Policy has invalid resource`, confirmez que le nom du compartiment dans la stratégie de compartiment correspond au nom de votre compartiment. Pour plus d'informations sur l'ajout d'une stratégie de compartiment, consultez [Comment puis-je ajouter une stratégie de compartiment S3 ?](#)

Si vous recevez un avertissement Error - Access denied (Erreur - Accès refusé) et que l'Éditeur de stratégie de compartiment ne vous permet pas d'enregistrer la stratégie de compartiment, vérifiez vos paramètres d'accès public au niveau du compte et du compartiment pour confirmer que vous autorisez l'accès public au compartiment.

## Étape 4 : Tester le point de terminaison de votre site web

Une fois que vous avez configuré votre compartiment en tant que site web statique et défini des autorisations, vous pouvez accéder à votre site web via un point de terminaison de site web Amazon S3. Pour de plus amples informations, veuillez consulter [Points de terminaison des sites web](#) dans le Amazon Simple Storage Service Manuel du développeur. Pour obtenir la liste complète des points de terminaison du site web Amazon S3, veuillez consulter [Points de terminaison du site web Amazon S3](#) dans le Référence générale d'Amazon Web Services.

## Comment rediriger toutes les demandes à un site web hébergé dans un compartiment S3 vers un autre hôte ?

Pour de plus amples informations sur la configuration d'une redirection dans Amazon S3, veuillez consulter [Configuration de la redirection de page web](#) dans le Amazon Simple Storage Service Manuel du développeur.

Vous pouvez rediriger toutes les demandes d'un point de terminaison de site Web pour un compartiment vers un autre hôte. Si vous redirigez toutes les demandes, chaque demande adressée au point de terminaison de site Web sera redirigée vers le nom d'hôte spécifié.

Par exemple, si votre domaine racine est `example.com`, et que vous souhaitez gérer des demandes pour `http://example.com` et `http://www.example.com`, vous pouvez créer deux compartiments nommés `example.com` et `www.example.com`. Ensuite, gérez le contenu dans le compartiment `example.com` et configurez l'autre compartiment `www.example.com` de manière à rediriger toutes les demandes vers

le compartiment `example.com`. Pour de plus amples informations, veuillez consulter les informations relatives à la [configuration d'un site Web statique à l'aide d'un nom de domaine personnalisé](#).

Pour rediriger des demandes pour un point de terminaison de site Web de compartiment

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez le nom du compartiment que vous avez configuré en tant que site web statique (par exemple `example.com`).
3. Choisissez Propriétés.
4. Choisissez Hébergement de site Web statique.
5. Choisissez Rediriger les demandes.
6. Dans la zone Target bucket or domain (Compartiment ou domaine cible) entrez le compartiment ou le domaine vers lequel vous souhaitez rediriger les demandes.

Par exemple, si vous redirigez les demandes vers une adresse de domaine racine, entrez **example.com**.

7. Dans la zone Protocol (Protocole) entrez le protocole pour les demandes redirigées (**http** ou **https**).
- Si vous ne spécifiez pas de protocole, le protocole de la demande d'origine est utilisé.
8. Choisissez Save.

## Paramètres avancés pour les propriétés de compartiment S3

Cette section explique comment configurer les paramètres avancés des propriétés de compartiment S3 pour la réplication d'objet, la notification d'événements et l'accélération de transfert.

### Rubriques

- [Comment configurer la destination des notifications d'événements ? \(p. 24\)](#)
- [Comment activer et configurer des notifications d'événements pour un compartiment S3 ? \(p. 26\)](#)
- [Comment activer Transfer Acceleration pour un compartiment S3 ? \(p. 31\)](#)

## Comment configurer la destination des notifications d'événements ?

Avant d'activer les notifications d'événement pour votre compartiment, vous devez configurer l'un des types de destination suivants :

### Une rubrique Amazon SNS

Amazon Simple Notification Service (Amazon SNS) est un service web qui coordonne et gère la mise à disposition ou l'envoi de messages à des clients ou à des points de terminaison abonnés. Vous pouvez utiliser la console Amazon SNS pour créer la rubrique Amazon SNS qui recevra vos notifications. La rubrique Amazon SNS doit être située dans la même région que votre compartiment Amazon S3. Pour plus d'informations sur la création d'une rubrique Amazon SNS, consultez [Mise en route](#) dans le manuel Amazon Simple Notification Service Manuel du développeur.

Pour pouvoir utiliser la rubrique Amazon SNS que vous créez comme destination d'une notification d'événement, vous devez disposer des éléments suivants :

- ARN (Amazon Resource Name) de la rubrique Amazon SNS

- Abonnement en cours de validité à la rubrique Amazon SNS (les abonnés à la rubrique reçoivent une notification lorsqu'un message est publié sur votre rubrique Amazon SNS)
- Stratégie d'autorisation définie dans la console Amazon SNS (comme illustré dans l'exemple suivant)

```
{
  "Version": "2012-10-17",
  "Id": "__example_policy_ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-number:topic-name",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:s3::bucket-name"
        }
      }
    }
  ]
}
```

#### Une file d'attente Amazon SQS

Vous pouvez utiliser la console Amazon SQS pour créer la file d'attente Amazon SQS qui recevra vos notifications. La file d'attente Amazon SQS doit être située dans la même région que votre compartiment Amazon S3. Pour plus d'informations sur la création d'une file d'attente Amazon SQS, consultez [Mise en route avec Amazon SQS](#) dans le manuel Amazon Simple Queue Service Manuel du développeur.

Pour pouvoir utiliser la file d'attente Amazon SQS en tant que destination d'une notification d'événement, vous devez disposer des éléments suivants :

- ARN (Amazon Resource Name) de la rubrique Amazon SQS
- Stratégie d'autorisation définie dans la console Amazon SQS (comme illustré dans l'exemple suivant)

```
{
  "Version": "2012-10-17",
  "Id": "__example_policy_ID",
  "Statement": [
    {
      "Sid": "example-statement-ID",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "SQS:*",
      "Resource": "arn:aws:sqs:region:account-number:queue-name",
      "Condition": {
        "ArnEquals": {
          "aws:SourceArn": "arn:aws:s3::bucket-name"
        }
      }
    }
  ]
}
```

#### Une fonction Lambda

Vous pouvez utiliser la console AWS Lambda pour créer une fonction Lambda. La fonction Lambda doit être située dans la même région que votre compartiment S3. Pour plus d'informations sur la création d'une fonction Lambda, consultez le manuel [AWS Lambda Developer Guide](#).

Pour pouvoir utiliser la fonction Lambda comme destination de la notification d'événement, vous devez disposer du nom ou de l'ARN d'une fonction Lambda pour configurer la fonction Lambda comme destination de la notification de l'événement.

#### Warning

Si votre notification finit par écrire dans le compartiment qui déclenche la notification, cela pourrait provoquer une boucle d'exécution. Par exemple, si le compartiment déclenche une fonction Lambda chaque fois qu'un objet est chargé et que la fonction charge un objet dans le compartiment, la fonction se déclenche elle-même indirectement. Afin d'éviter cela, utilisez deux compartiments ou configurez le déclencheur pour qu'il s'applique uniquement à un préfixe utilisé pour les objets entrants.

Pour plus d'informations et un exemple d'utilisation Amazon S3 des notifications avec AWS Lambda, consultez [Utilisation d'AWS Lambda avec Amazon S3](#) dans le AWS Lambda Developer Guide.

## Comment activer et configurer des notifications d'événements pour un compartiment S3 ?

Vous pouvez autoriser certains événements Amazon S3 à envoyer un message de notification à une destination chaque fois qu'ils se produisent. Cette section explique comment utiliser la console Amazon S3 pour activer les notifications d'événements. Pour plus d'informations sur l'utilisation des notifications d'événements avec les kits SDK AWS et les API REST Amazon S3, consultez [Configuration des notifications pour les événements Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

#### Rubriques

- [Types de notifications d'événements](#) (p. 26)
- [Destinations de la notification d'événement](#) (p. 27)
- [Activation et configuration des notifications d'événements](#) (p. 28)
- [Plus d'informations](#) (p. 31)

## Types de notifications d'événements

Lorsque vous configurez des notifications d'événements pour un compartiment, vous devez spécifier le type d'événements pour lesquels vous souhaitez recevoir des notifications. Pour obtenir la liste complète des types d'événements, consultez [Types d'événements pris en charge](#) dans le Amazon Simple Storage Service Manuel du développeur.

La console Amazon S3 propose les options suivantes pour configurer les notifications d'événements. Vous pouvez choisir une ou plusieurs options.

- Date de création de l'objet
  - Tous les événements de création d'objet – Recevez une notification lorsqu'un objet est créé dans votre compartiment par l'une des actions de création d'objet suivantes : Put, Post, Copy et Chargement partitionné terminé.
  - Put, Post, Copy et Chargement partitionné terminé – Recevez une notification pour l'une de ces actions de création d'objet spécifiques.
- Suppression d'objets
  - Tous les événements de suppression d'objet – Recevez une notification chaque fois qu'un objet de votre compartiment est supprimé.
  - Création d'un marqueur de suppression – Recevez une notification lorsqu'un marqueur de suppression est créé pour un objet versionné.

Pour obtenir des informations sur la suppression d'objets versionnés, consultez [Suppression des versions d'objet](#). Pour obtenir des informations sur la gestion des versions d'un objet, consultez [Gestion des versions d'un objet](#) et [Utilisation de la gestion des versions](#).

- Restauration d'objets à partir de S3 Glacier ou de la classe de stockage S3 Glacier Deep Archive
  - Restauration lancée – Recevez une notification pour le lancement de la restauration d'objets.
  - Restauration achevée – Recevez une notification pour l'achèvement de la restauration d'objets.
- Un événement de perte d'un objet Reduced Redundancy Storage (RRS)
  - Objet dans RSS perdu – Recevez une notification indiquant qu'un objet de la classe de stockage RRS a été perdu.
- Objets éligibles à la réplication à l'aide du contrôle du temps de réplication Amazon S3
  - Seuil de réplication manqué – Recevez une notification indiquant qu'un objet a dépassé le seuil de 15 minutes pour la réplication.
  - Temps de réplication terminé après le seuil – Recevez une notification indiquant qu'un objet a répliqué après le seuil de 15 minutes.
  - Temps de réplication non suivi – Recevez une notification indiquant qu'un objet éligible à la réplication n'est plus suivi par les mesures de réplication.
  - Échec du seuil de réplication – Recevez une notification en cas d'échec de la réplication d'un objet.

#### Note

Lorsque vous supprimez le dernier objet d'un dossier, Amazon S3 peut générer un événement de création d'objet. Lorsqu'il existe plusieurs objets comportant le même préfixe avec une barre oblique (/) dans leurs noms, ces objets sont affichés comme faisant partie d'un dossier dans la console Amazon S3. Le nom du dossier est constitué des caractères qui précèdent la barre oblique (/).

Lorsque vous supprimez tous les objets répertoriés sous ce dossier, il n'existe aucun objet réel disponible pour représenter le dossier vide. Dans ces circonstances, la console Amazon S3 crée un objet de zéro octet pour représenter ce dossier. Si vous avez activé la notification d'événements pour la création d'objets, l'action de création d'un objet de zéro octet qui est entreprise par la console va déclencher un événement de création de l'objet.

La console Amazon S3 affiche un dossier dans les circonstances suivantes :

- Lorsque le nom d'un objet zéro octet contient une barre oblique (/). Dans ce cas, il y a un objet Amazon S3 réel de 0 octets qui représente un dossier.
- Si le nom de l'objet contient une barre oblique (/). Dans ce cas, il n'y a pas d'objet réel représentant le dossier.

## Destinations de la notification d'événement

Lorsque vous configurez des notifications d'événements pour un compartiment, vous choisissez également la destination de la notification. Des messages de notification d'événement peuvent être envoyés aux destinations suivantes :

- Rubrique Amazon Simple Notification Service (Amazon SNS) – Coordonne et gère la diffusion ou l'envoi de messages aux points de terminaison ou aux clients abonnés. Pour obtenir des informations sur le format des rubriques Amazon SNS, consultez [FAQ SNS](#).
- File d'attente Amazon Simple Queue Service (Amazon SQS) – Offre des files d'attente hébergées fiables et scalables dédiées au stockage des messages pendant leur transit entre les ordinateurs. Pour plus d'informations sur Amazon SQS, consultez [Qu'est-ce qu'Amazon Simple Queue Service ?](#) dans le Amazon Simple Queue Service Manuel du développeur.
- AWS Lambda – Invoque une fonction Lambda et fournit le message d'événement en tant qu'argument. Lorsque vous créez une fonction Lambda, vous empaquetez et téléchargez votre code personnalisé vers



AWS Lambda. AWS Lambda utilise l'infrastructure AWS pour exécuter le code en votre nom. Pour plus d'informations sur l'utilisation de Lambda avec Amazon S3, consultez [Utilisation d'AWS Lambda avec Amazon S3](#) dans le manuel AWS Lambda Developer Guide.

Pour plus d'informations sur l'octroi au principal du service Amazon S3 des autorisations requises pour la publication de notifications d'événement vers une destination, consultez [Octroi d'autorisations pour la publication de messages de notification d'événement vers une destination](#) dans le Guide du développeur Amazon S3.

#### Warning

Si votre notification finit par écrire dans le compartiment qui déclenche la notification, cela pourrait provoquer une boucle d'exécution. Par exemple, si le compartiment déclenche une fonction Lambda chaque fois qu'un objet est chargé et que la fonction charge un objet dans le compartiment, la fonction se déclenche elle-même indirectement. Afin d'éviter cela, utilisez deux compartiments ou configurez le déclencheur pour qu'il s'applique uniquement à un préfixe utilisé pour les objets entrants.

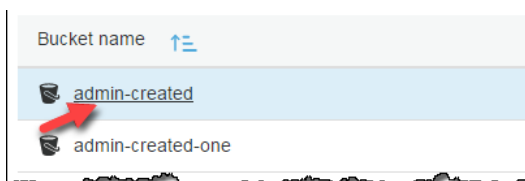
Pour plus d'informations et un exemple d'utilisation Amazon S3 des notifications avec AWS Lambda, consultez [Utilisation d'AWS Lambda avec Amazon S3](#) dans le AWS Lambda Developer Guide.

## Activation et configuration des notifications d'événements

Avant d'activer les notifications d'événements pour votre compartiment, vous devez configurer l'un de ces types de destination. Pour de plus amples informations, veuillez consulter [Comment configurer la destination des notifications d'événements ?](#) (p. 24)

Pour activer et configurer des notifications d'événements pour un compartiment S3

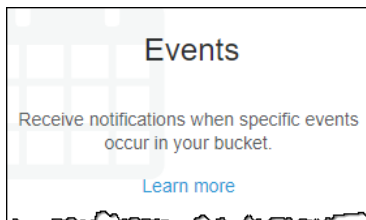
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez activer les événements.



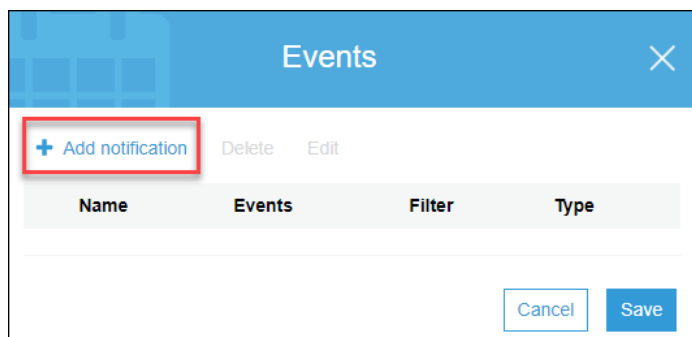
3. Choisissez Properties.



4. Sous Paramètres avancés, choisissez Événements.

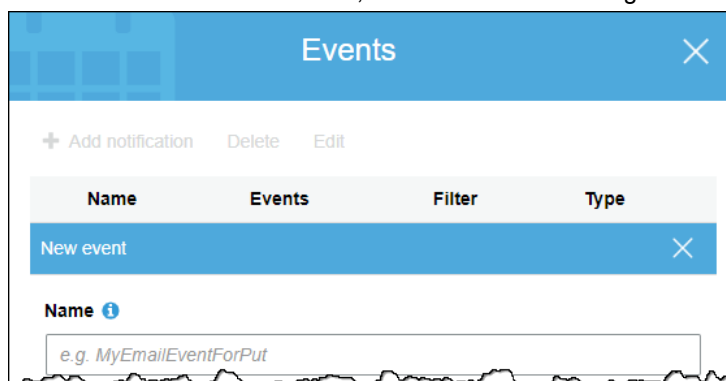


5. Choisissez Ajouter une notification.



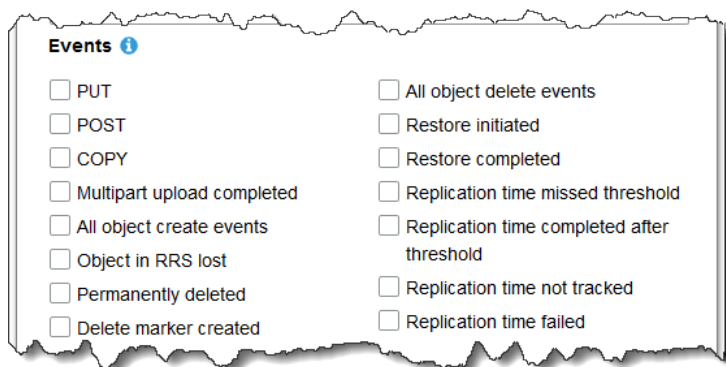
6. Dans le champ Name (Nom), saisissez un nom décrivant la notification de votre événement.

Si vous ne saisissez aucun nom, un identifiant GUID est généré et utilisé pour le nom.



7. Sous Events (Événements), sélectionnez un ou plusieurs événements.

Pour obtenir la liste des types d'événements, consultez [Types de notifications d'événements \(p. 26\)](#).



8. Pour filtrer les notifications d'événements par un préfixe ou un suffixe, saisissez un Prefix (Préfixe) ou un Suffix (Suffixe).

Par exemple, vous pouvez configurer un filtre de préfixe de sorte à recevoir uniquement des notifications lorsque des fichiers sont ajoutés à un dossier spécifique (par exemple, `images/`). Pour plus d'informations, consultez [Configuration des notifications à l'aide du filtrage par nom de clé d'objet](#).

The screenshot shows two input fields. The first is labeled 'Prefix' with a blue information icon and contains the text 'e.g. images/'. The second is labeled 'Suffix' with a blue information icon and contains the text 'e.g. .jpg'.

9. Choisissez la destination de notification d'événement : SNS Topic (Rubrique SNS), SQS Queue (File d'attente SQS), ou Lambda Function (Fonction Lambda).

Pour obtenir une description des destinations, consultez [Destinations de la notification d'événement \(p. 27\)](#).

The screenshot shows a 'Send to' section with a dropdown menu. The dropdown is open, showing 'Select notification destination' as the selected option. Below the dropdown is a 'Cancel' button and a 'Save' button.

Lorsque vous choisissez votre destination Envoyer à, une boîte de dialogue apparaît pour vous permettre de saisir votre destination de fonction SNS, SQS ou Lambda spécifique. Dans l'exemple ci-dessous, l'emplacement Send To (Envoyer à) est SNS Topic (Rubrique SNS), et vous pouvez voir une boîte SNS pour le nom de rubrique SNS.

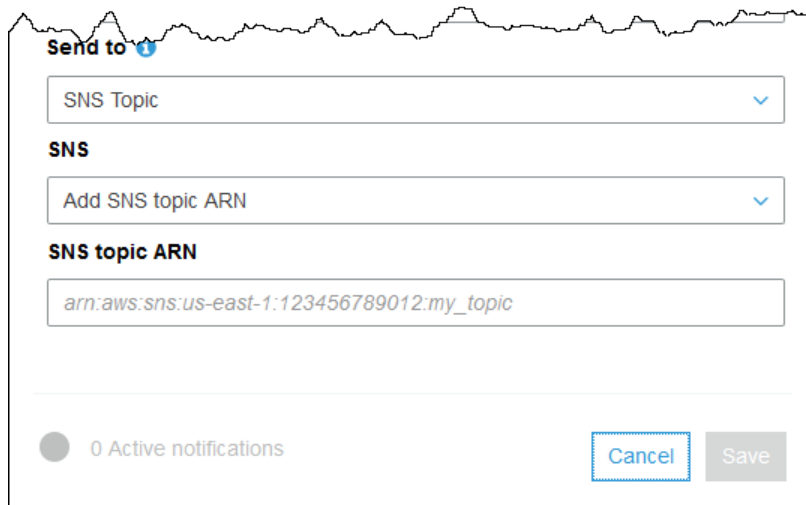
The screenshot shows a 'Send to' dialog box. The 'Send to' dropdown is set to 'SNS Topic'. Below it, there is an 'SNS' section with a dropdown menu for selecting the SNS topic.

10. Dans la boîte qui apparaît, choisissez ou saisissez la fonction SNS, SQS ou Lambda de destination.

Vous pouvez choisir ou entrer le nom de la fonction SNS, SQS ou Lambda, ou choisir le nom de l'Amazon Resource Name (ARN) de destination. L'exemple de capture d'écran ci-dessous montre l'option Add SNS topic ARN (Ajouter l'ARN de la rubrique SNS).

The screenshot shows the same 'Send to' dialog box as before, but with an additional button at the bottom labeled 'Add SNS topic ARN'.

11. Si vous avez choisi Add ARN (Ajouter un ARN), saisissez la rubrique SNS, la file d'attente SQS ou l'ARN de la fonction Lambda.



Send to ⓘ

SNS Topic

**SNS**

Add SNS topic ARN

**SNS topic ARN**

arn:aws:sns:us-east-1:123456789012:my\_topic

0 Active notifications

Cancel Save

12. Choisissez Enregistrer.

Amazon S3 envoie un message de test à la destination de la notification d'événement.

## Plus d'informations

- [Comment restaurer un objet S3 qui a été archivé ? \(p. 51\)](#)

## Comment activer Transfer Acceleration pour un compartiment S3 ?

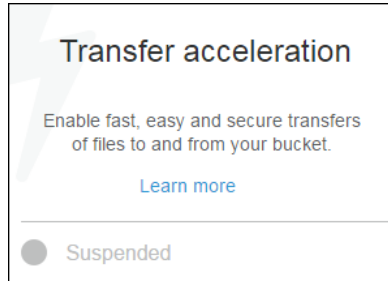
Amazon Simple Storage Service (Amazon S3) Transfer Acceleration permet un transfert rapide, facile et sécurisé de fichiers entre votre client et un compartiment S3 sur de longues distances. Cette rubrique explique comment activer Amazon S3 Transfer Acceleration pour un compartiment. Pour plus d'informations, consultez [Amazon S3 Transfer Acceleration](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour activer Transfer Acceleration pour un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Compartiments, choisissez le nom du compartiment pour lequel vous souhaitez activer Transfer Acceleration.
3. Choisissez Properties.



4. Sous Paramètres avancés, choisissez Transfer Acceleration.

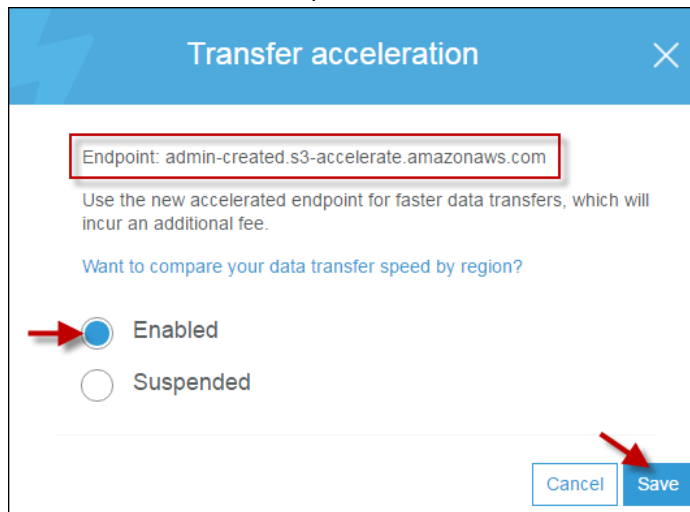


5. (Facultatif) Si vous souhaitez comparer des vitesses de téléchargement accélérées et non accélérées, pour ouvrir l' [outil de comparaison de vitesse Amazon S3 Transfer Acceleration](#) , choisissez l'option Souhaitez-vous comparer la vitesse de transfert de vos données par région ?.

L'outil de comparaison de vitesse utilise les chargements partitionnés pour transférer un fichier à partir de votre navigateur vers différentes régions AWS avec ou sans Transfer Acceleration d'Amazon S3. Vous pouvez comparer la vitesse de téléchargement des téléchargements directs et transférer des téléchargements accélérés par région.

6. Choisissez Activé, puis Enregistrer.

Point de terminaison affiche le point de terminaison Transfer Acceleration de votre compartiment. Vous utilisez ce point de terminaison pour accéder à des transferts de données accélérés vers et depuis votre compartiment. Si vous interrompez Transfer Acceleration, le point de terminaison de l'accélération ne fonctionne plus.



# Présentation des points d'accès Amazon S3

Vous pouvez utiliser les points d'accès Amazon S3 pour gérer l'accès à vos objets S3. Les points d'accès Amazon S3 sont des points de terminaison réseau nommés qui sont associés à des compartiments que vous pouvez utiliser pour effectuer des opérations d'objet S3, telles que le chargement et la récupération d'objets. Un compartiment peut avoir jusqu'à 1 000 points d'accès qui lui sont associés et chaque point d'accès applique des autorisations et des contrôles réseau distincts pour vous donner un contrôle précis sur l'accès à vos objets S3.

Pour plus d'informations sur les points d'accès Amazon S3, consultez [Gestion de l'accès aux données avec des points d'accès Amazon S3](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Les rubriques suivantes expliquent comment utiliser la console de gestion S3 pour créer, gérer et utiliser des points d'accès Amazon S3.

## Rubriques

- [Création d'un point d'accès \(p. 33\)](#)
- [Gestion et utilisation des points d'accès Amazon S3 \(p. 34\)](#)

## Création d'un point d'accès

Cette section explique comment créer un point d'accès Amazon S3 à l'aide de la AWS Management Console. Pour plus d'informations sur la création de points d'accès à l'aide de l'AWS CLI, des kits SDK AWS et des API REST Amazon S3, consultez [Gestion de l'accès aux données avec des points d'accès Amazon S3](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Un point d'accès est associé à un seul compartiment Amazon S3. Avant de commencer, assurez-vous d'avoir créé le compartiment que vous souhaitez utiliser avec ce point d'accès. Pour plus d'informations sur la création de compartiments, consultez [Création et configuration d'un compartiment S3 \(p. 3\)](#).

### Pour créer un point d'accès

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la section Compartiments S3, sélectionnez le compartiment que vous souhaitez associer à ce point d'accès.
3. Sur la page détaillée du compartiment, choisissez l'onglet Access points (Points d'accès).
4. Choisissez Create access point (Créer un point d'accès).
5. Entrez le nom souhaité pour le point d'accès dans le champ Access point name (Nom du point d'accès).
6. Choisissez un type d'accès réseau. Si vous choisissez Virtual Private Cloud (VPC), entrez l'ID VPC que vous souhaitez utiliser avec le point d'accès.

Pour plus d'informations sur le type d'accès réseau pour les points d'accès, consultez [Création de points d'accès restreints à un virtual private cloud](#) dans le Amazon Simple Storage Service Manuel du développeur.

7. Sélectionnez les paramètres de blocage d'accès public que vous souhaitez appliquer au point d'accès. Tous les paramètres de blocage d'accès public sont activés par défaut pour les nouveaux points

d'accès, et nous vous recommandons de laisser tous les paramètres activés sauf si vous savez que vous avez un besoin spécifique de désactiver l'un d'entre eux. Actuellement, Amazon S3 ne prend pas en charge la modification des paramètres de blocage d'accès public d'un point d'accès une fois ce dernier créé.

Pour plus d'informations sur l'utilisation du blocage d'accès public Amazon S3 avec des points d'accès, consultez [Gestion de l'accès public aux points d'accès](#) dans le Amazon Simple Storage Service Manuel du développeur.

8. (Facultatif) Spécifiez la stratégie de point d'accès. La console affiche automatiquement le nom Amazon Resource Name (ARN) du point d'accès, que vous pouvez utiliser dans la stratégie.
9. Choisissez Create access point (Créer un point d'accès).

## Gestion et utilisation des points d'accès Amazon S3

Cette section explique comment gérer et utiliser vos points d'accès Amazon S3 à l'aide de l'AWS Management Console. Chaque point d'accès est associé à un seul compartiment Amazon S3. Avant de commencer, accédez à la liste de vos points d'accès pour un compartiment, comme décrit dans la procédure suivante.

Pour rechercher une liste de points d'accès pour un compartiment

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la section S3 buckets (Compartiments S3), sélectionnez le compartiment dont vous souhaitez gérer les points d'accès.
3. Sur la page détaillée du compartiment, choisissez l'onglet Access points (Points d'accès).

Dans l'onglet Access points (Points d'accès) vous pouvez afficher les détails de configuration d'un point d'accès, modifier la stratégie d'un point d'accès, utiliser un point d'accès pour accéder à votre compartiment ou supprimer un point d'accès. Les procédures suivantes expliquent comment effectuer chacune de ces tâches.

Pour afficher les détails de la configuration d'un point d'accès

1. Accédez à l'onglet Access points (Points d'accès) de votre compartiment.
2. Localisez le point d'accès dont vous souhaitez afficher la configuration. Vous pouvez rechercher le point d'accès dans la liste de points d'accès ou rechercher un point d'accès spécifique à l'aide du champ Search by name (Rechercher par nom).
3. Choisissez le nom du point d'accès dont vous souhaitez afficher la configuration.

### Note

Pour afficher la configuration d'un point d'accès, choisissez (cliquez sur) le nom du point d'accès et non le bouton d'option situé à côté du nom du point d'accès.

Pour modifier une stratégie de point d'accès

1. Accédez à l'onglet Access points (Points d'accès) de votre compartiment.
2. Sélectionnez le bouton d'option en regard du nom du point d'accès dont vous souhaitez modifier la stratégie.
3. Choisissez Edit access point policy (Modifier la stratégie de point d'accès).
4. Entrez la stratégie dans le champ de texte. La console affiche automatiquement le nom Amazon Resource Name (ARN) du point d'accès, que vous pouvez utiliser dans la stratégie. Vous pouvez

également choisir Générateur de stratégies pour utiliser le Générateur de stratégies AWS afin de vous aider à élaborer la stratégie.

5. Choisissez Enregistrer.

#### Pour utiliser un point d'accès afin d'accéder à votre compartiment

1. Accédez à l'onglet Access points (Points d'accès) de votre compartiment.
2. Sélectionnez le bouton d'option en regard du nom du point d'accès que vous souhaitez utiliser.
3. Choisissez Use this access point (Utiliser ce point d'accès).
4. La console affiche une étiquette au-dessus du nom de votre compartiment qui indique le point d'accès que vous utilisez actuellement. Lorsque vous utilisez le point d'accès, vous ne pouvez effectuer que les opérations d'objet permises par les autorisations du point d'accès.

##### Note

La vue de la console affiche toujours tous les objets du compartiment. L'utilisation d'un point d'accès comme cette procédure le décrit limite les opérations que vous pouvez effectuer sur ces objets, mais pas si vous pouvez voir qu'ils existent dans le compartiment.

5. Pour quitter la vue du point d'accès de votre compartiment, choisissez Exit access point (Quitter le point d'accès).

##### Note

La console de gestion S3 ne prend pas en charge l'utilisation de points d'accès Virtual Private Cloud (VPC) pour accéder aux ressources de compartiment. Pour accéder aux ressources de compartiment à partir d'un point d'accès VPC, utilisez les SDK AWS CLI ou AWS, ou les API REST Amazon S3.

#### Pour supprimer un point d'accès

1. Accédez à l'onglet Access points (Points d'accès) de votre compartiment.
2. Sélectionnez le bouton d'option en regard du nom du point d'accès à supprimer.
3. Sélectionnez Supprimer.
4. Confirmez que vous souhaitez supprimer votre point d'accès en entrant son nom dans le champ de texte qui s'affiche, puis choisissez Confirmer.



# Chargement, téléchargement et gestion d'objets

Pour charger vos données (photos, vidéos, documents, etc.) dans Amazon S3, vous devez d'abord créer un compartiment S3 dans l'une des régions AWS. Vous pouvez ensuite charger un nombre illimité d'objets de données dans ce compartiment.

Les objets désignent les données que vous stockez dans Amazon S3. Chaque objet réside dans un compartiment que vous créez au sein d'une région AWS spécifique. Chaque objet que vous stockez dans Amazon S3 réside dans un compartiment.

Les objets stockés dans une région ne quittent jamais la région, à moins que vous ne les transfériez explicitement vers une autre région. Par exemple, les objets stockés dans la région Europe (Irlande) ne la quittent jamais. Les objets stockés physiquement dans une région AWS restent dans cette région. Amazon S3 ne garde pas de copie des objets ou les déplace vers d'autres régions. Toutefois, vous pouvez accéder aux objets depuis n'importe où, à condition de disposer des autorisations nécessaires.

Avant que vous ne puissiez charger un objet dans Amazon S3, vous devez disposer des autorisations en écriture dans un compartiment.

Les objets peuvent correspondre à tout type de fichier : images, sauvegardes, données, films, etc. Vous pouvez disposer d'un nombre illimité d'objets dans un compartiment. La taille maximale de fichier que vous pouvez télécharger à l'aide de la console Amazon S3 est de 160 Go. Pour charger un fichier d'une taille supérieure à 160 Go, utilisez l'CLI AWS, le kit SDK AWS ou l'API REST Amazon S3. Pour en savoir plus, consultez [Téléchargement d'objets](#) dans le Amazon Simple Storage Service Manuel du développeur.

Les rubriques suivantes expliquent comment utiliser la console Amazon S3 pour charger, supprimer et gérer des objets.

## Note

Si vous renommez un objet ou modifiez l'une des propriétés suivantes, Storage Class, Encryption et Metadata, un nouvel objet est créé pour remplacer l'ancien. Si l'option Gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

## Rubriques

- [Comment charger des fichiers ou des dossiers dans un compartiment S3 ? \(p. 37\)](#)
- [Copier un objet \(p. 45\)](#)
- [Déplacement d'un objet \(p. 45\)](#)
- [Comment télécharger un objet à partir d'un compartiment S3 ? \(p. 46\)](#)
- [Comment supprimer des objets d'un compartiment S3 ? \(p. 49\)](#)
- [Comment restaurer un objet S3 supprimé ? \(p. 50\)](#)
- [Comment restaurer un objet S3 qui a été archivé ? \(p. 51\)](#)
- [Comment verrouiller un objet Amazon S3 ? \(p. 56\)](#)
- [Comment afficher la présentation d'un objet ? \(p. 58\)](#)
- [Comment afficher les versions d'un objet S3 ? \(p. 61\)](#)
- [Comment afficher les propriétés d'un objet ? \(p. 62\)](#)
- [Comment ajouter le chiffrement à un objet S3 ? \(p. 64\)](#)
- [Comment ajouter des métadonnées à un objet S3 ? \(p. 67\)](#)

- [Comment ajouter des balises à un objet S3 ? \(p. 73\)](#)
- [Comment utiliser les dossiers d'un compartiment S3 ? \(p. 75\)](#)

## Comment charger des fichiers ou des dossiers dans un compartiment S3 ?

Cette rubrique explique comment utiliser AWS Management Console pour charger un ou plusieurs fichiers ou des dossiers entiers dans un compartiment Amazon S3. Avant de pouvoir charger des fichiers ou des dossiers vers un compartiment Amazon S3, vous devez disposer d'autorisations en écriture pour le compartiment. Pour plus d'informations sur les autorisations d'accès, consultez [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#). Pour plus d'informations sur le chargement de fichiers par programmation, consultez [Chargement d'objets](#) dans le Amazon Simple Storage Service Manuel du développeur.

Lorsque vous chargez un fichier vers Amazon S3, il est stocké en tant qu'objet S3. Les objets se composent des données du fichier et des métadonnées décrivant l'objet. Vous pouvez disposer d'un nombre illimité d'objets dans un compartiment.

Vous pouvez charger n'importe quel type de fichier (images, sauvegardes, données, films, etc.) dans un compartiment S3. La taille maximale d'un fichier que vous pouvez télécharger à l'aide de la console Amazon S3 est de 160 Go. Pour charger un fichier d'une taille supérieure à 160 Go, utilisez la CLI AWS, le kit SDK AWS ou l'API REST Amazon S3. Pour en savoir plus, consultez [Téléchargement d'objets](#) dans le Amazon Simple Storage Service Manuel du développeur.

### Note

Pour charger des dossiers, vous devez les faire glisser et les déposer. Pour télécharger des fichiers, vous pouvez les faire glisser et les déposer, ou pointer et cliquer. La fonctionnalité de glisser-déposer est prise en charge uniquement pour les navigateurs Chrome et Firefox.

Pour de plus amples informations sur les versions prises en charge des navigateurs Chrome et Firefox, veuillez consulter [Quels navigateurs sont pris en charge et peuvent être utilisés avec l'AWS Management Console ?](#).

Lorsque vous chargez un dossier, Amazon S3 charge tous les fichiers et sous-dossiers du dossier spécifié dans le compartiment. Ensuite, il attribue un nom de clé d'objet qui combine le nom du fichier chargé et le nom du dossier. Par exemple, si vous chargez un dossier appelé `/images` qui contient deux fichiers, `sample1.jpg` et `sample2.jpg`, Amazon S3 charge les fichiers et attribue ensuite les noms de clé correspondants, `images/sample1.jpg` et `images/sample2.jpg`. Les noms de clé incluent le nom de dossier comme préfixe. La console Amazon S3 affiche uniquement la partie du nom de clé qui suit le dernier signe « / ». Par exemple, dans un dossier `images`, les objets `images/sample1.jpg` et `images/sample2.jpg` s'affichent sous la forme `sample1.jpg` et `sample2.jpg`.

Si vous chargez des fichiers individuels et si un dossier est ouvert dans la console Amazon S3, lorsqu'Amazon S3 charge les fichiers, il inclut le nom du dossier ouvert comme préfixe des noms de clé. Par exemple, si vous avez un objet appelé `backup` ouvert dans la console Amazon S3 et si vous chargez un fichier appelé `sample1.jpg`, le nom de clé est `backup/sample1.jpg`. Cependant, l'objet s'affiche dans la console en tant que `sample1.jpg` dans le dossier `backup`.

Si vous chargez des fichiers individuels et si aucun dossier n'est ouvert dans la console Amazon S3, lorsqu'Amazon S3 charge les fichiers, il affecte uniquement le nom de fichier comme nom de clé. Par exemple, si vous chargez un fichier appelé `sample1.jpg`, le nom de clé est `sample1.jpg`. Pour plus d'informations sur les noms de clés, consultez [Clé d'objet et métadonnées](#) dans le Amazon Simple Storage Service Manuel du développeur.

Si vous chargez un objet avec un nom de clé qui existe déjà dans un compartiment pour lequel la gestion des versions est activé, Amazon S3 crée une autre version de l'objet au lieu de remplacer l'objet existant.

Pour plus d'informations sur la gestion des versions, consultez [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#).

#### Rubriques

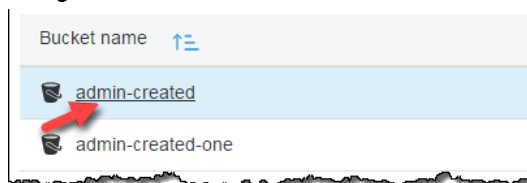
- [Chargement de fichiers et de dossiers par glisser-déposer \(p. 38\)](#)
- [Chargement de fichiers en pointant et en cliquant \(p. 43\)](#)
- [Plus d'informations \(p. 44\)](#)

## Chargement de fichiers et de dossiers par glisser-déposer

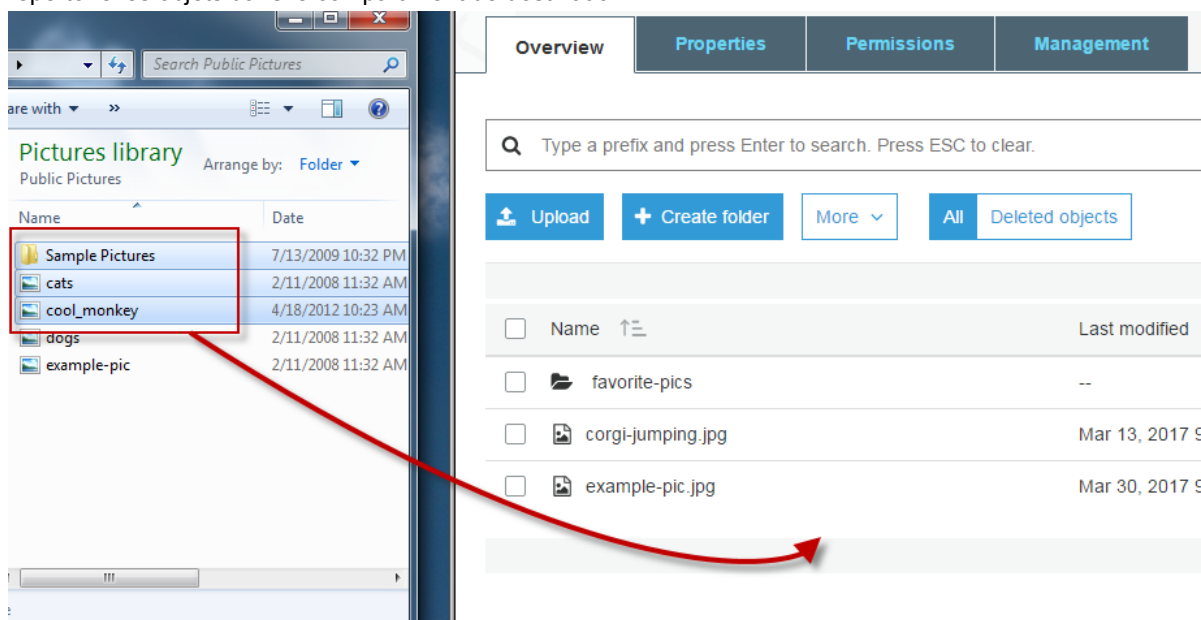
Si vous utilisez les navigateurs Chrome ou Firefox, vous pouvez choisir les dossiers et fichiers à charger, puis les faire glisser et les déposer dans le compartiment de destination. L'opération de glisser-déposer est le seul moyen de charger des dossiers.

Pour charger des dossiers et des fichiers vers un compartiment S3 par glisser-déposer

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment dans lequel vous souhaitez charger vos dossiers ou fichiers.

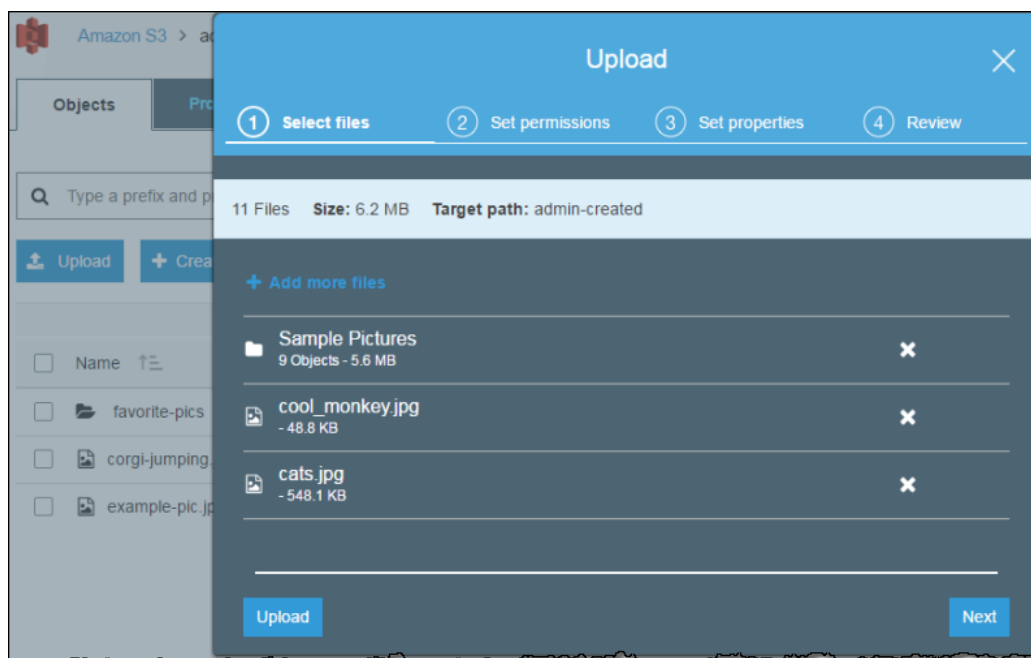


3. Dans une fenêtre autre que celle de la console, sélectionnez les fichiers et dossiers que vous souhaitez charger. Puis faites glisser vos sélections et déposez-les dans la fenêtre de la console qui répertorie les objets dans le compartiment de destination.



Les fichiers que vous avez choisis sont répertoriés dans la boîte de dialogue Charger.

4. Dans la boîte de dialogue Charger, exécutez l'une des actions suivantes :
  - a. Faites glisser davantage de fichiers et dossiers et déposez-les dans la fenêtre de la console qui affiche la boîte de dialogue Charger. Pour ajouter d'autres fichiers, vous pouvez également choisir Ajouter des fichiers supplémentaires. Cette option fonctionne uniquement pour des fichiers, pas pour des dossiers.
  - b. Pour charger immédiatement les fichiers et dossiers répertoriés sans octroyer ni supprimer d'autorisations pour des utilisateurs spécifiques, ni définir d'autorisations publiques pour tous les fichiers que vous chargez, choisissez Charger. Pour plus d'informations sur les autorisations d'accès aux objets, consultez [Comment définir les autorisations d'un objet ? \(p. 124\)](#).
  - c. Pour définir des autorisations ou propriétés pour les fichiers que vous chargez, choisissez Suivant.



5. Sur la page Définir des autorisations, sous Gérer les utilisateurs, vous pouvez modifier les autorisations dont bénéficie le propriétaire du compte AWS. Le propriétaire désigne l'utilisateur racine du compte AWS et non un utilisateur AWS Identity and Access Management (IAM). Pour en savoir plus sur l'utilisateur racine, consultez [Utilisateur racine d'un compte AWS](#).

Choisissez Ajouter un compte pour accorder l'accès à un autre compte AWS. Pour plus d'informations sur l'accord d'autorisations à un autre compte AWS, consultez [Comment définir des autorisations de compartiment ACL ? \(p. 127\)](#).

Sous Gérer les autorisations publiques, vous pouvez octroyer des droits d'accès en lecture sur vos objets au grand public (tout le monde), pour tous les fichiers que vous chargez. L'octroi de l'accès en lecture public est applicable à un petit sous-ensemble de cas d'utilisation, par exemple, lorsque des compartiments sont utilisés pour des sites web. Nous vous recommandons de ne pas modifier le paramétrage par défaut de l'option Ne pas octroyer d'accès en lecture public à ces objets. Vous pourrez toujours modifier les autorisations associées à un objet après son chargement. Pour plus d'informations sur les autorisations d'accès aux objets, consultez [Comment définir les autorisations d'un objet ? \(p. 124\)](#).

Lorsque vous avez terminé de configurer les autorisations, choisissez Suivant.

Upload

1 Files Size: 1.3 MB Target path: admin-created

Manage users

User ID	Objects	Object permissions
johndoe(Owner)	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write	<input checked="" type="checkbox"/> Read <input checked="" type="checkbox"/> Write

Access for other AWS account [+ Add account](#)

Account Objects Object permissions

Manage public permissions

Do not grant public read access to this object(s) (Recommended)

Upload Previous Next

6. Sur la page Définir les propriétés, choisissez la méthode de classe de stockage et de chiffrement à utiliser pour les fichiers que vous chargez. Vous pouvez également ajouter ou modifier les métadonnées.
  - a. Choisissez une classe de stockage pour les fichiers que vous chargez. Pour plus d'informations sur les classes de stockage, consultez [Classes de stockage](#) dans le Amazon Simple Storage Service Manuel du développeur.

Upload

1 Select files 2 Set permissions 3 Set properties 4 Review

Storage class

Choose a storage class based on your use case and access requirements. [Learn more](#) or see [Amazon S3 pricing](#)

Storage class	Designed for	Availability Zones	Min storage duration	Min billable object size	Monitoring and automation fees	Retrieval fees
<input type="radio"/> Standard	Frequently accessed data	≥ 3	-	-	-	-
<input checked="" type="radio"/> Intelligent-Tiering	Long-lived data with changing or unknown access patterns	≥ 3	30 days	-	Per-object fees apply	-
<input type="radio"/> Standard-IA	Long-lived, infrequently accessed data	≥ 3	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> One Zone-IA	Long-lived, infrequently accessed, non-critical data	≥ 1	30 days	128KB	-	Per-GB fees apply
<input type="radio"/> Glacier	Archive data with retrieval times ranging from minutes to hours	≥ 3	90 days	-	-	Per-GB fees apply
<input type="radio"/> Glacier Deep Archive	Archive data that rarely, if ever, needs to be accessed	≥ 3	180 days	-	-	Per-GB fees apply

Upload Previous Next

- b. Choisissez le type de chiffrement à utiliser pour les fichiers que vous chargez. Si vous ne souhaitez pas les chiffrer, choisissez Aucun.

- i. Pour chiffrer les fichiers chargés à l'aide de clés gérées par Amazon S3, choisissez Amazon S3 master-key (Clé principale Amazon S3). Pour plus d'informations, consultez [Protection des données avec des clés de chiffrement gérées par Amazon S3](#) dans Amazon Simple Storage Service Manuel du développeur.
- ii. Pour chiffrer les fichiers chargés avec AWS Key Management Service (AWS KMS), choisissez AWS KMS master-key (Clé principale AWS KMS). Puis, choisissez une clé CMK dans la liste des clés CMK AWS KMS.

#### Note

Pour chiffrer des objets dans un compartiment, vous pouvez uniquement utiliser les clés disponibles dans la même région AWS que le compartiment.

Vous pouvez permettre à un compte externe d'utiliser un objet protégé par une clé CMK AWS KMS. Pour ce faire, sélectionnez ARN KMS personnalisé dans la liste et saisissez l'Amazon Resource Name (ARN) du compte externe. Les administrateurs d'un compte externe qui disposent des autorisations d'utilisation sur un objet protégé par la clé AWS KMS peuvent ensuite restreindre l'accès en créant une stratégie IAM au niveau des ressources.

Pour plus d'informations sur la création d'une clé CMK AWS KMS, consultez [Création de clés](#) dans le AWS Key Management Service Developer Guide. Pour plus d'informations sur la protection des données avec AWS KMS, consultez [Protection des données avec les clés stockées dans AWS KMS \(SSE-KMS\)](#) dans le Amazon Simple Storage Service Manuel du développeur.

- c. Les métadonnées d'objet Amazon S3 sont représentées par une paire nom-valeur (clé-valeur). Il existe deux types de métadonnées : les métadonnées définies par le système et définies par l'utilisateur.

Si vous voulez ajouter des métadonnées définies par le système Amazon S3 à tous les objets que vous chargez, pour En-tête, sélectionnez un en-tête. Vous pouvez sélectionner des en-têtes HTTP communs, tels que Content-Type (Type de contenu) et Disposition-contenu. Saisissez une valeur pour l'en-tête, puis choisissez Enregistrer. Pour obtenir la liste des métadonnées définies par le système et pour savoir si vous pouvez ajouter la valeur, consultez [Métadonnées définies par le système](#) dans le Amazon Simple Storage Service Manuel du développeur.

- d. Toute métadonnée commençant par un préfixe `x-amz-meta-` est traitée comme une métadonnée définie par l'utilisateur. Les métadonnées définies par l'utilisateur sont stockées avec l'objet et renvoyées une fois que vous avez téléchargé l'objet.

Pour ajouter des métadonnées définies par l'utilisateur à tous les objets que vous chargez, saisissez `x-amz-meta-` ainsi que le nom des métadonnées personnalisées dans le champ En-tête. Saisissez une valeur pour l'en-tête, puis choisissez Enregistrer. Les clés et leurs valeurs doivent respecter les normes US-ASCII. Les métadonnées définies par l'utilisateur peuvent atteindre 2 Ko. Pour plus d'informations sur les métadonnées définies par l'utilisateur, consultez [Métadonnées définies par l'utilisateur](#) dans le Amazon Simple Storage Service Manuel du développeur.

Metadata

Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.

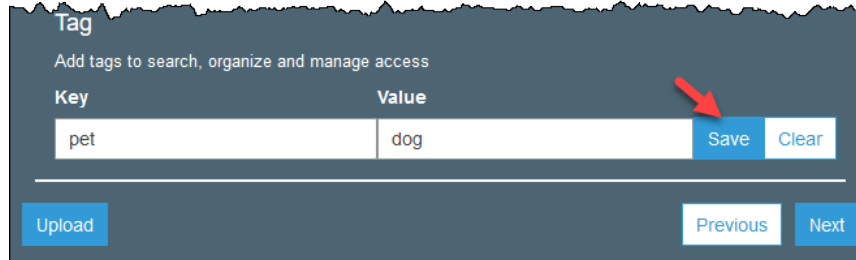
Header	Value
x-amz-meta-my-data-1	myUserDefinedMetada

Save Clear

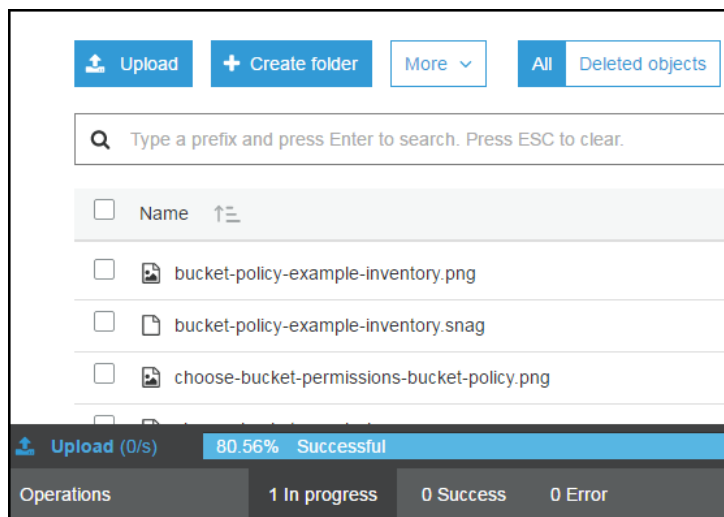
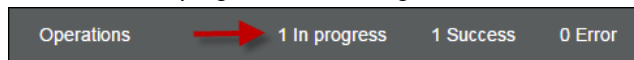
Tag

- e. Le balisage des objets vous permet de classer le stockage par catégorie. Chaque balise est une paire clés-valeurs. Les valeurs de clés et de balises sont sensibles à la casse. Vous pouvez avoir jusqu'à 10 balises par objet.

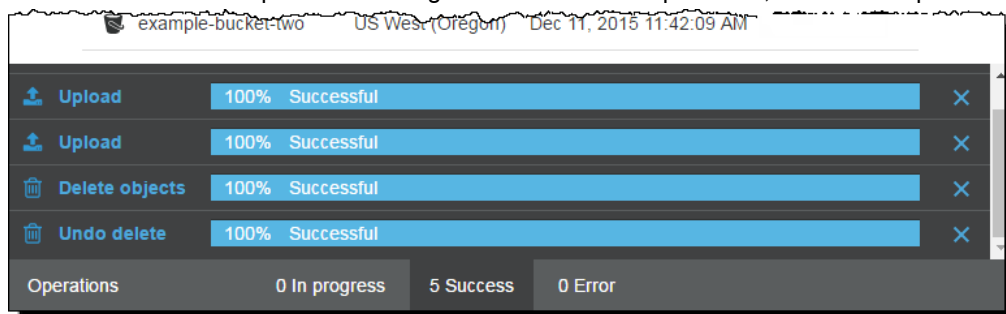
Pour ajouter des balises à tous les objets que vous chargez, entrez le nom d'une balise dans le champ Clé. Saisissez une valeur pour la balise, puis choisissez Enregistrer. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 255 caractères Unicode. Pour plus d'informations sur les balises d'objets, consultez [Balisage des objets](#) dans le Amazon Simple Storage Service Manuel du développeur.



7. Choisissez Suivant.
8. Sur la page de vérification Charger, vérifiez que les paramètres sont corrects, puis choisissez Charger. Pour effectuer des modifications, sélectionnez Précédent.
9. Pour afficher la progression du chargement, choisissez En cours en bas de la fenêtre du navigateur.



Pour afficher un historique de vos chargements et d'autres opérations, choisissez Opération réussie.

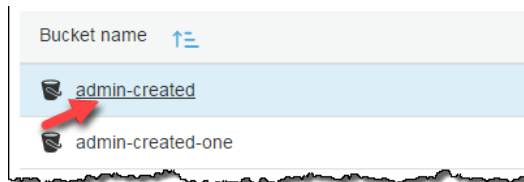


## Chargement de fichiers en pointant et en cliquant

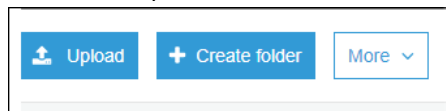
Cette procédure explique comment charger des fichiers dans un compartiment S3 à l'aide de l'option Charger.

Pour charger les fichiers vers un compartiment S3 en pointant et en cliquant

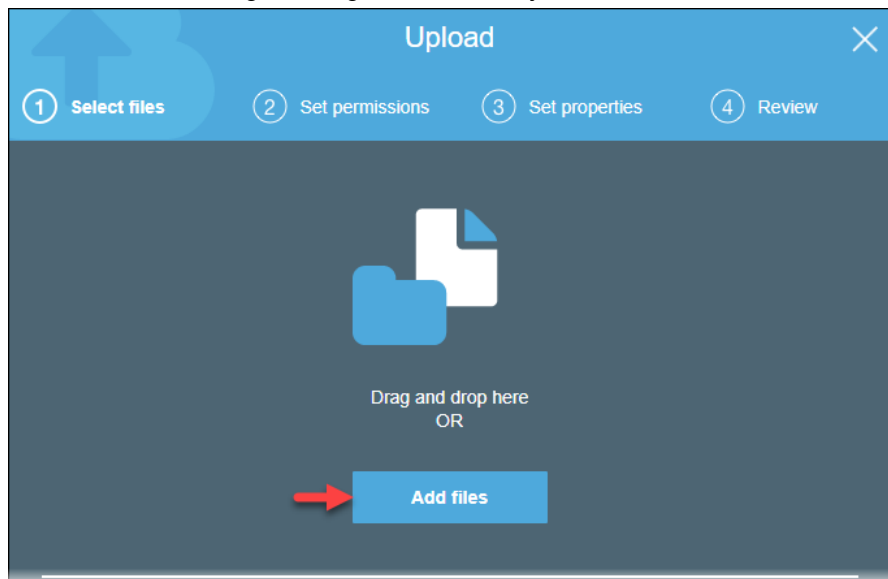
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment dans lequel vous souhaitez charger vos fichiers.



3. Choisissez Upload.

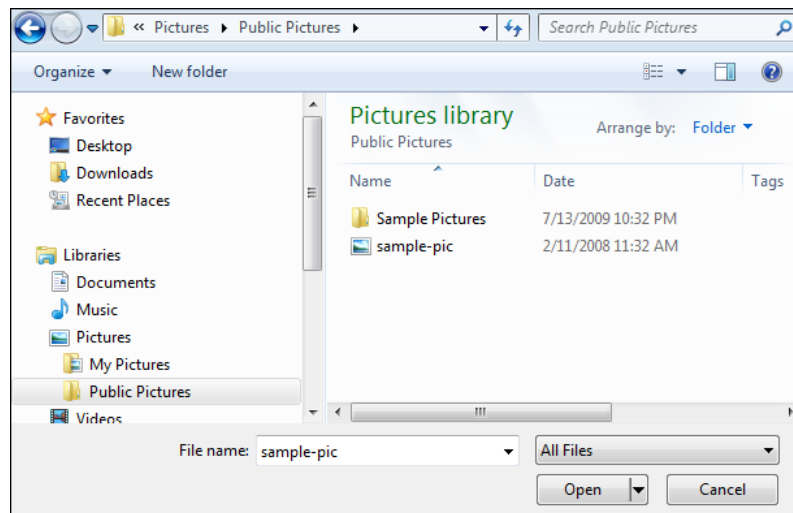


4. Dans la boîte de dialogue Charger, choisissez Ajouter des fichiers.

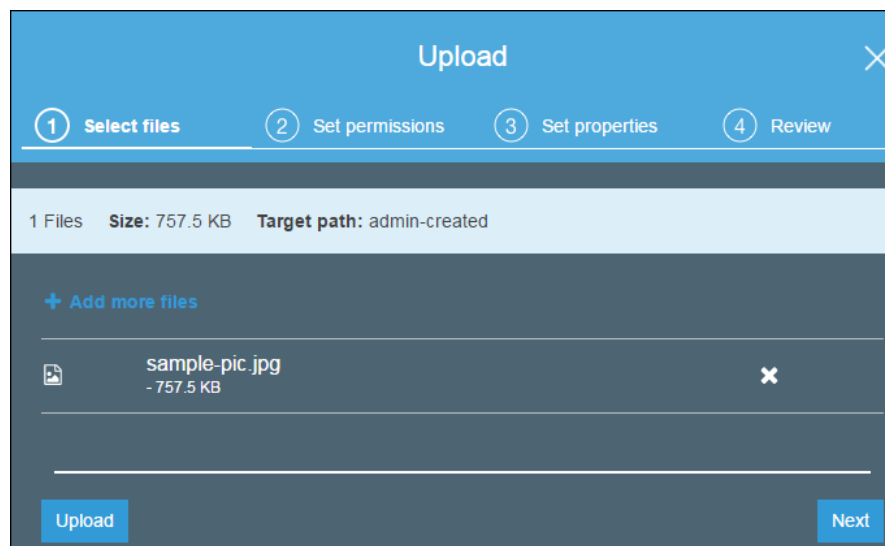


5. Choisissez un ou plusieurs fichiers à charger, puis choisissez Ouvrir.





6. Lorsque les fichiers que vous avez choisis sont répertoriés dans la boîte de dialogue Charger, exécutez l'une des actions suivantes :
- Pour ajouter d'autres fichiers, choisissez Ajouter des fichiers supplémentaires.
  - Pour charger immédiatement les fichiers répertoriés, choisissez Charger.
  - Pour définir des autorisations ou propriétés pour les fichiers que vous chargez, choisissez Suivant.



7. Pour définir des autorisations et des propriétés, commencez à l'Étape 5 de la rubrique [Chargement de fichiers et de dossiers par glisser-déposer](#) (p. 38).

## Plus d'informations

- [Comment définir les autorisations d'un objet ?](#) (p. 124).
- [Comment télécharger un objet à partir d'un compartiment S3 ?](#) (p. 46)

## Copier un objet

Dans la console Amazon S3, vous pouvez copier un objet dans un compartiment ou dans un dossier. Pour plus d'informations, veuillez consulter [Copie d'objets](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour copier un objet

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Compartiments, choisissez le nom de votre compartiment.
3. Dans l'onglet Présentation, activez la case à cocher en regard de l'objet que vous souhaitez copier.
4. Choisissez Actions, puis Copier.
5. Choisissez la destination de la copie :
  - Si vous souhaitez copier votre objet dans un compartiment, sélectionnez ce dernier.
  - Si vous souhaitez copier votre objet dans le dossier d'un compartiment, choisissez le nom du compartiment, puis choisissez le dossier.
6. Sous Réviser, confirmez les détails de la copie, puis choisissez Copier.

Amazon S3 copie votre objet dans la destination.

### Note

Cette action copie tous les objets spécifiés. Lorsque vous copiez des dossiers, attendez la fin de l'action de copie pour apporter des modifications supplémentaires dans les dossiers.

## Déplacement d'un objet

Dans la console Amazon S3, vous pouvez déplacer un objet vers un compartiment ou un dossier.

Pour déplacer un objet

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Compartiments, choisissez le nom de votre compartiment.
3. Activez la case à cocher en regard de l'objet que vous souhaitez déplacer.
4. Choisissez Actions, puis Déplacer.
5. Choisissez la destination du déplacement :
  - Si vous souhaitez déplacer votre objet vers un compartiment, sélectionnez ce dernier.
  - Si vous souhaitez déplacer votre objet vers un dossier dans un compartiment, choisissez le nom du compartiment, puis choisissez le dossier.
6. Sous Révision, confirmez les détails du déplacement, puis choisissez Déplacer.

Amazon S3 déplace votre objet vers la destination.

### Note

Cette action déplace tous les objets spécifiés. Lorsque vous déplacez des dossiers, attendez la fin de l'action de déplacement pour apporter des modifications supplémentaires dans les dossiers.

## Comment télécharger un objet à partir d'un compartiment S3 ?

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

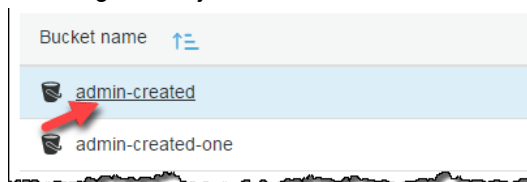
Des frais de transfert de données s'appliquent lorsque vous téléchargez des objets. Pour plus d'informations sur les fonctionnalités et la tarification d'Amazon S3, consultez [Amazon S3](#).

### Important

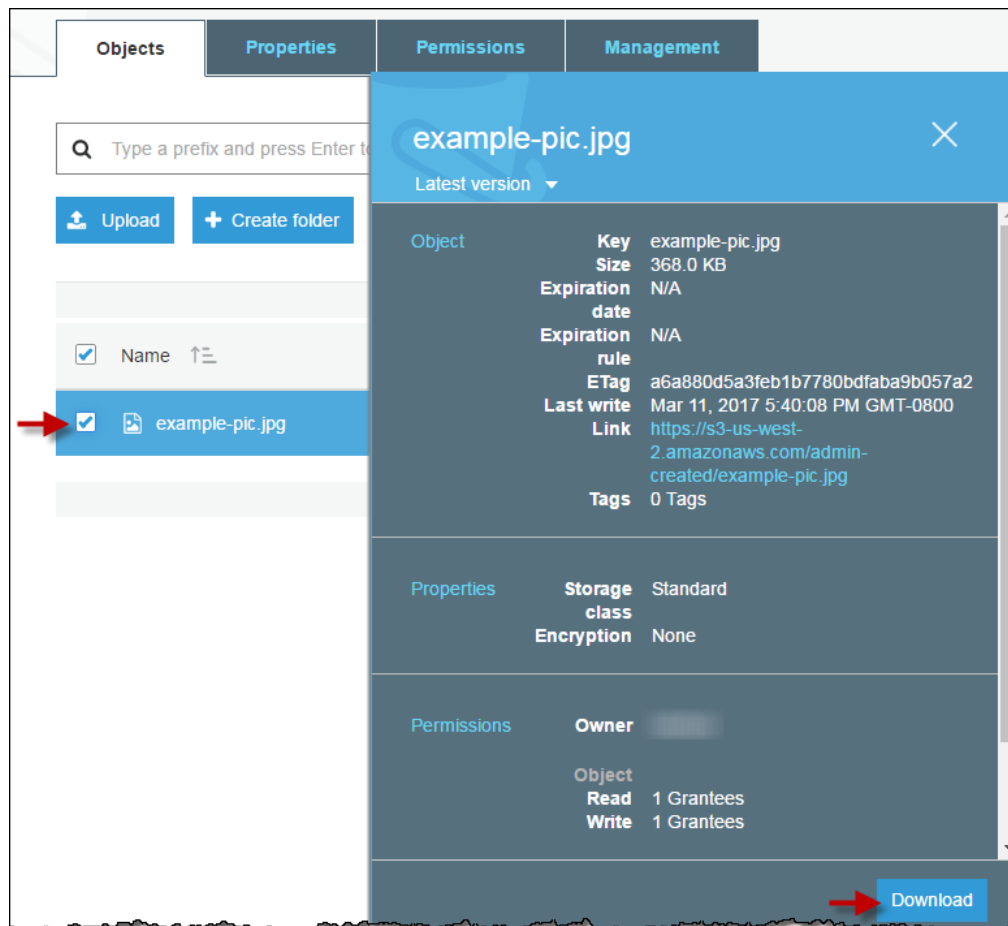
- Si un nom de clé d'objet est composé d'un point unique (.) ou de deux points (..), vous ne pouvez pas télécharger l'objet à l'aide de la console Amazon S3. Pour télécharger un objet avec un nom de clé de « . » ou « .. », vous devez utiliser l'AWS CLI, les kits SDK AWS ou les API REST. Pour plus d'informations sur la dénomination des objets, consultez [Directives de désignation de clés d'objets](#) dans le Amazon Simple Storage Service Manuel du développeur.
- Vous pouvez télécharger un seul objet par requête à l'aide de la console Amazon S3. Pour [télécharger plusieurs objets, utilisez la AWS CLI, le kit AWS SDK ou l'API REST](#).

Pour télécharger un objet à partir d'un compartiment S3

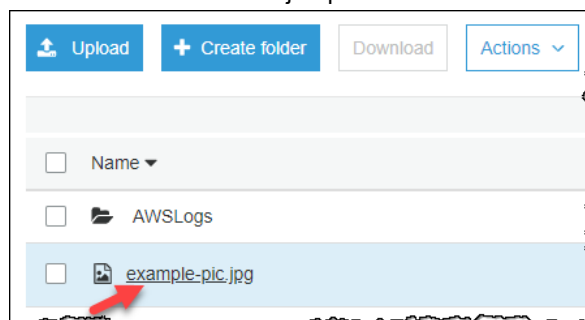
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment à partir duquel vous souhaitez télécharger un objet.



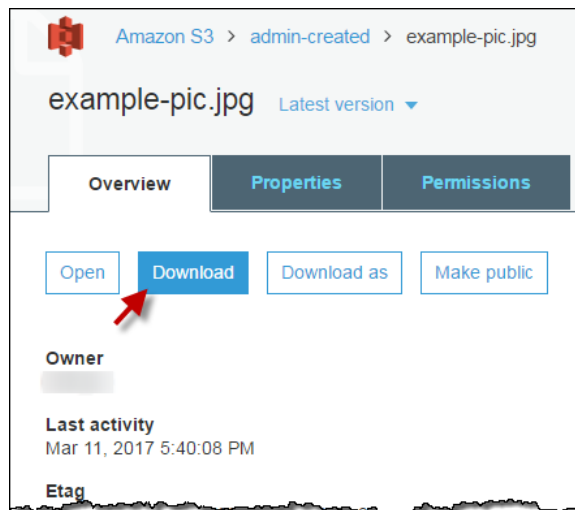
3. Vous pouvez télécharger un objet à partir d'un compartiment S3 de l'une des façons suivantes :
  - Dans la liste Nom, sélectionnez la case à cocher en regard de l'objet que vous souhaitez télécharger, puis choisissez Télécharger sur la page de description de l'objet qui s'affiche.



- Choisissez le nom de l'objet que vous souhaitez télécharger.



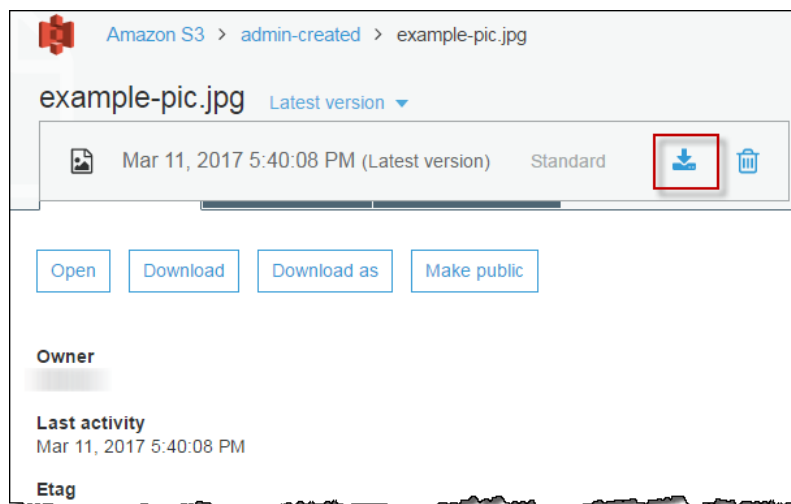
Sur la page Présentation, choisissez Télécharger.



- Choisissez le nom de l'objet que vous souhaitez télécharger, puis Télécharger en tant que sur la page Présentation.



- Choisissez le nom de l'objet que vous souhaitez télécharger. Choisissez Dernière version, puis cliquez sur l'icône de téléchargement.



## Voir aussi

- [Comment charger des fichiers ou des dossiers dans un compartiment S3 ? \(p. 37\)](#)

## Comment supprimer des objets d'un compartiment S3 ?

Cette section explique comment utiliser la console Amazon S3 pour supprimer des objets. Etant donné que tous les objets dans le compartiment S3 entraînent des coûts de stockage, vous devez supprimer ceux dont vous n'avez plus besoin. Si vous collectez des fichiers journaux, par exemple, vous pouvez les supprimer lorsque vous n'en avez plus besoin. Vous pouvez configurer une règle de cycle de vie pour supprimer automatiquement les objets tels que les fichiers journaux.

Pour plus d'informations sur les fonctionnalités et la tarification d'Amazon S3, consultez [Amazon S3](#).

Pour supprimer des objets d'un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment à partir duquel vous souhaitez supprimer un objet.
3. Vous pouvez supprimer des objets d'un compartiment S3 de l'une des façons suivantes :
  - Dans la liste Nom, sélectionnez la case à cocher en regard des objets et des dossiers que vous souhaitez supprimer, choisissez Actions, puis Supprimer dans le menu déroulant.

Dans la boîte de dialogue Supprimer les objets, vérifiez que le ou les noms des objets et des dossiers que vous avez sélectionnés en vue de leur suppression sont répertoriés, puis choisissez Supprimer.

- Choisissez le nom de l'objet que vous souhaitez supprimer, choisissez Dernière version, puis choisissez l'icône de corbeille.

### Warning

Cette action supprime tous les objets spécifiés. Lorsque vous supprimez des dossiers, attendez la fin de l'action de suppression pour ajouter de nouveaux objets au dossier. Dans le cas contraire, de nouveaux objets pourraient également être supprimés.

## Plus d'informations

- [Comment restaurer un objet S3 supprimé ? \(p. 50\)](#)
- [Comment créer la stratégie de cycle de vie d'un compartiment S3 ? \(p. 83\)](#)

## Comment restaurer un objet S3 supprimé ?

Cette section explique comment utiliser la console Amazon S3 pour récupérer (restaurer) des objets supprimés.

Pour pouvoir restaurer un objet supprimé, la gestion des versions doit être activée sur le compartiment qui contient l'objet avant la suppression de l'objet. Pour plus d'informations sur l'activation de la gestion des versions, consultez [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#).

Lorsque vous supprimez un objet d'un compartiment activé pour la gestion des versions, toutes les versions restent dans le compartiment et Amazon S3 crée un marqueur de suppression pour l'objet. Pour annuler la suppression de l'objet, vous devez supprimer ce marqueur de suppression. Pour en savoir plus sur la gestion des versions et la suppression des marqueurs, consultez [Gestion des versions d'un objet](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Pour récupérer des objets supprimés à partir d'un compartiment S3

Les étapes suivantes expliquent comment récupérer des objets supprimés qui ne sont pas des dossiers de votre compartiment S3, y compris les objets qui se trouvent dans ces dossiers.

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.
3. Pour accéder à une liste des versions d'un objet du compartiment, sélectionnez Afficher. Vous pourrez voir les marqueurs de suppression pour les objets supprimés.
4. Pour annuler la suppression d'un objet, vous devez supprimer le marqueur de suppression. Cochez la case en regard du marqueur de suppression de l'objet à récupérer, puis choisissez Supprimer dans le menu Actions.
5. Choisissez ensuite Masquer. L'objet dont la suppression a été annulée apparaît alors dans la liste.

### Note

Vous ne pouvez pas utiliser la console Amazon S3 pour annuler les dossiers. Vous devez utiliser l'interface de ligne de commande AWS ou un kit SDK. Consultez par exemple [Comment récupérer un objet Amazon S3 qui a été supprimé dans un compartiment pour lequel la gestion des versions est activée ?](#)

## Plus d'informations

- [Comment afficher les versions d'un objet S3 ? \(p. 61\)](#)
- [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#)

- [Utilisation de la gestion des versions](#) dans le manuel Amazon Simple Storage Service Manuel du développeur

## Comment restaurer un objet S3 qui a été archivé ?

Cette section explique comment utiliser la console Amazon S3 pour restaurer un objet qui a été archivé à l'aide des classes de stockage S3 Glacier ou S3 Glacier Deep Archive. Les objets stockés dans S3 Glacier ou S3 Glacier Deep Archive ne sont pas immédiatement accessibles. Pour accéder à un objet dans cette classe, vous devez en restaurer une copie temporaire à son compartiment S3 pour la durée (en jours) que vous spécifiez. Pour plus d'informations sur les classes de stockage S3 Glacier ou S3 Glacier Deep Archive, consultez [Classes de stockage](#) dans le Amazon Simple Storage Service Manuel du développeur.

Lorsque vous restaurez une archive, vous payez pour l'archive et pour la copie restaurée. En raison des coûts de stockage associés à la copie, il est préférable de restaurer les objets uniquement pour la durée nécessaire. Si vous souhaitez une copie permanente de l'objet, créez-en une copie dans votre compartiment S3. Pour plus d'informations sur les fonctionnalités et la tarification d'Amazon S3, consultez [Amazon S3](#).

Une fois un objet restauré, vous pouvez le télécharger à partir de la page Présentation. Pour plus d'informations, consultez [Comment afficher la présentation d'un objet ? \(p. 58\)](#).

### Rubriques

- [Options de récupération des archives \(p. 51\)](#)
- [Restauration d'un objet S3 archivé \(p. 52\)](#)
- [La mise à niveau est une restauration en cours \(p. 54\)](#)
- [Vérification du statut de la restauration et de la date d'expiration de l'archive \(p. 55\)](#)

## Options de récupération des archives

Voici les opérations relatives aux options de récupération lors de la restauration d'un objet archivé :

- **Expedited** - Les récupérations accélérées vous permettent d'accéder rapidement à vos données stockées dans la classe de stockage S3 Glacier lorsque des demandes urgentes occasionnelles concernant un sous-ensemble d'archives sont nécessaires. Pour tous les objets archivés à l'exception des plus volumineux (plus de 250 Mo), les données auxquelles vous accédez à l'aide des récupérations rapides sont généralement disponibles en 1 à 5 minutes. La capacité provisionnée garantit que la capacité des récupérations rapides est disponible lorsque vous en avez besoin. Pour plus d'informations, consultez [Capacité allouée](#). Les récupérations accélérées et la capacité provisionnée ne sont pas disponibles pour les objets stockés dans la classe de stockage S3 Glacier Deep Archive.
- **Standard** - Les récupérations Standard vous permettent d'accéder à vos objets archivés en quelques heures. C'est l'option par défaut pour les demandes de récupération S3 Glacier ou S3 Glacier Deep Archive qui ne spécifient pas l'option de récupération. Les récupérations standard se terminent généralement en 3 à 5 heures pour les objets stockés dans la classe de stockage S3 Glacier. Elles se terminent généralement en 12 heures pour les objets stockés dans la classe de stockage S3 Glacier Deep Archive.
- **Bulk** - Les récupérations en bloc constituent l'option de récupération Amazon S3 Glacier la moins onéreuse. Elles vous permettent de récupérer de grandes quantités de données (parfois des pétaoctets) à moindre coût. Les récupérations en bloc se terminent généralement en 5 à 12 heures pour les objets stockés dans la classe de stockage S3 Glacier. Elles se terminent généralement en 48 heures pour les objets stockés dans la classe de stockage S3 Glacier Deep Archive.

Pour plus d'informations sur les options de récupération, consultez [Restauration d'objets archivés](#) dans le Amazon Simple Storage Service Manuel du développeur.

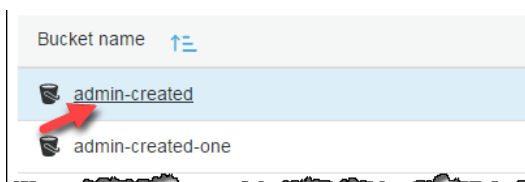


## Restauration d'un objet S3 archivé

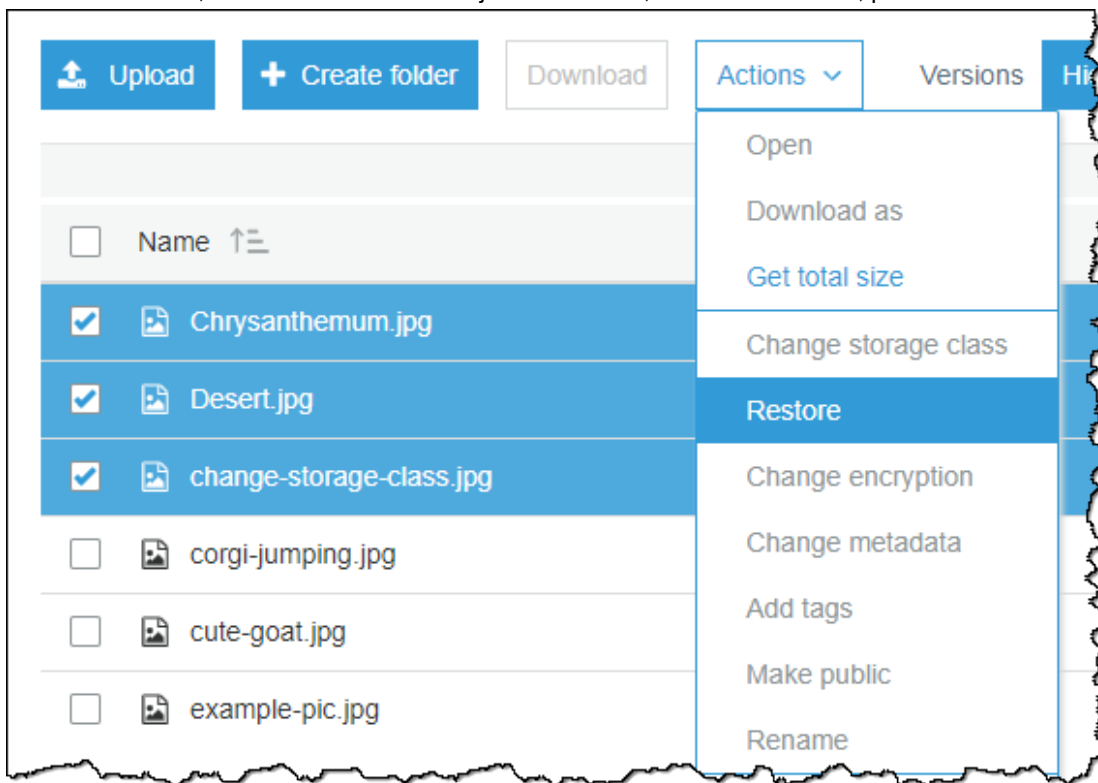
Cette rubrique explique comment utiliser la console Amazon S3 pour restaurer un objet qui a été archivé dans les classes de stockage S3 Glacier ou S3 Glacier Deep Archive. (La console utilise les noms Glacier et Glacier Deep Archive pour ces classes de stockage.)

Pour restaurer des objets S3 archivés

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient les objets que vous souhaitez restaurer.



3. Dans la liste Nom, sélectionnez le ou les objets à restaurer, choisissez Actions, puis Restaurer.



4. Dans la boîte de dialogue Commencer la restauration, saisissez le nombre de jours durant lesquels vous souhaitez que vos données archivées soient accessibles.
5. Choisissez l'une des options de récupération suivantes dans le menu Options de récupération.
  - Choisissez Bulk retrieval (Récupération en bloc) ou Standard retrieval (Récupération standard), puis Restaurer.
  - Choisissez Expedited retrieval (Récupération accélérée) (disponible uniquement pour la classe de stockage Glacier).

## Restore

Restored copies in the Reduced Redundancy Storage (RRS) are automatically deleted after the specified number of days. Retrieval fees apply. See [S3 pricing](#)

### Restore objects from Glacier

**Total objects:** 1  
**Total size:** 15.6 KB

**Number of days the restored copy is available**

days

Available until approximately 2019-04-05

**Restore tier**

☒ Bulk retrieval  
Typically within 5-12 hours

☐ Standard retrieval  
Typically within 3 - 5 hours

☐ Expedited retrieval  
Typically within 1 - 5 minutes when retrieving less than 250MB

CancelRestore

6. La capacité provisionnée est uniquement disponible pour la classe de stockage Glacier. Si vous disposez d'une capacité allouée, choisissez Restaurer pour lancer une récupération avec allocation. Si vous disposez d'une capacité allouée, toutes vos récupérations rapides sont transmises par le biais de votre capacité allouée. Pour plus d'informations sur la capacité allouée, consultez [Capacité allouée](#).
- Si vous ne disposez pas d'une capacité allouée et si vous ne voulez pas en acheter, choisissez Restaurer pour lancer une récupération à la demande.
  - Si vous ne disposez pas d'une capacité allouée, mais si vous souhaitez en acheter, choisissez Ajouter une unité de capacité, puis Acheter. Lorsque le message Réussite de l'achat s'affiche, choisissez Restaurer pour lancer une récupération avec allocation.

☒ Expedited retrieval  
Typically within 1 - 5 minutes when retrieving less than 250MB

**Purchased capacity units: 0**

[Add 1 capacity unit](#)

**Purchase 1 provisioned capacity unit.**

You will be immediately charged for each provisioned capacity unit and the purchase is not refundable. See [S3 pricing](#)

Provisioned capacity ensures that retrieval capacity for expedited retrievals is available when you need it. Each unit of capacity provides that at least three expedited retrievals can be performed every five minutes and provides up to 150 MB/s of retrieval throughput.

Once purchased, provisioned capacity units will be available for your use in the current region for one month from the date of purchase.

[Purchase](#)

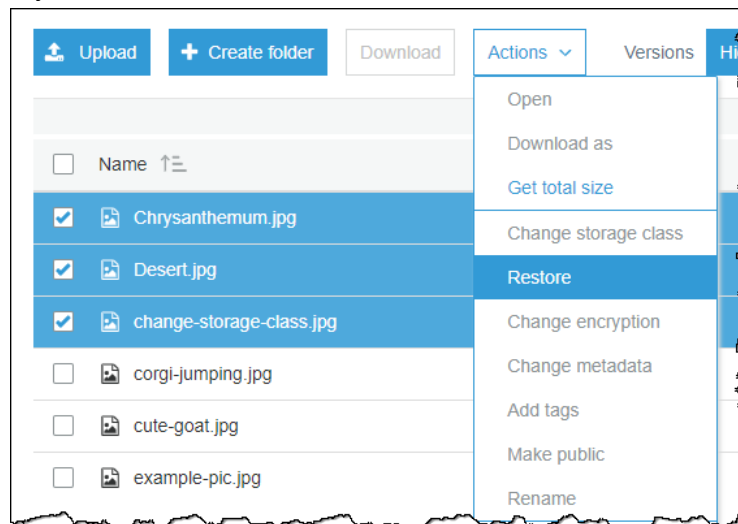
[Cancel](#) [Restore](#)

## La mise à niveau est une restauration en cours

Vous pouvez mettre à niveau la vitesse de la restauration pendant que cette dernière est en cours.

Pour mettre à niveau une restauration en cours vers un niveau plus rapide

1. Dans la liste Nom, sélectionnez un ou plusieurs objets que vous restaurez et choisissez Actions, puis Restaurer depuis Glacier. Pour plus d'informations sur la vérification du statut de restauration d'un objet, consultez [Vérification du statut de la restauration et de la date d'expiration de l'archive](#) (p. 55).



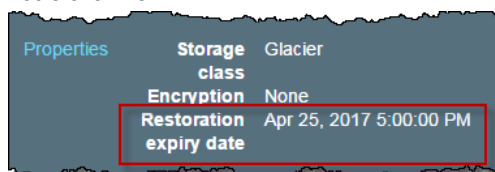
2. Choisissez le niveau auquel vous souhaitez passer, puis choisissez Restaurer. Pour plus d'informations sur la mise à niveau vers un niveau plus rapide, consultez [Restauration d'objets archivés](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Vérification du statut de la restauration et de la date d'expiration de l'archive

Pour contrôler la progression de la restauration, consultez le panneau de présentation de l'objet. Pour plus d'informations sur le panneau de présentation, consultez [Comment afficher la présentation d'un objet ?](#) (p. 58).

La section Présentation indique que la restauration est à l'état En cours.

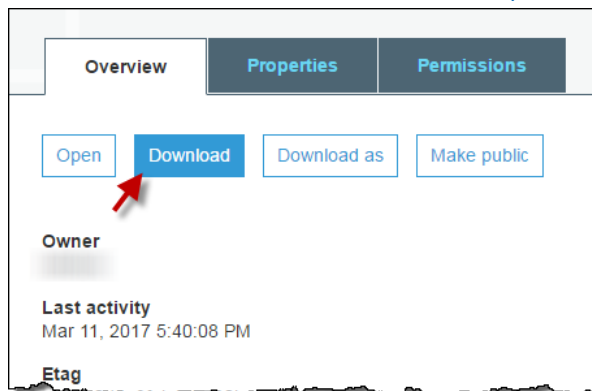
Lorsque la copie temporaire de l'objet est disponible, la section Présentation de l'objet indique Date d'expiration de la restauration. Cela indique à quel moment Amazon S3 supprimera la copie restaurée de votre archive.



Les objets restaurés sont stockés uniquement pendant le nombre de jours que vous spécifiez. Si vous souhaitez une copie permanente de l'objet, créez-en une copie dans votre compartiment Amazon S3.

Amazon S3 calcule la date d'expiration en ajoutant le nombre de jours que vous spécifiez à l'heure où vous demandez de restaurer l'objet, puis arrondit au jour suivant à minuit UTC. Ce calcul s'applique à la restauration initiale de l'objet et à chaque extension de la disponibilité que vous demandez. Par exemple, si un objet a été restauré le 15/10/2012 à 10 h 30 UTC et le nombre de jours spécifié est de 3, l'objet est donc disponible jusqu'au 19/10/2012 à 00 h 00 UTC. Si le 16/10/2012 à 11 h 00 UTC, vous remplacez le nombre de jours durant lesquels vous souhaitez qu'il soit accessible par 1, Amazon S3 rend l'objet disponible jusqu'au 18/10/2012 à 00 h 00 UTC.

Une fois un objet restauré, vous pouvez le télécharger à partir de la page Présentation. Pour plus d'informations, consultez [Comment afficher la présentation d'un objet ?](#) (p. 58).



## Plus d'informations

- [Restauration d'objets archivés](#) dans le manuel du développeur Amazon S3.

- [restore-object](#) dans la référence de commande AWS CLI.
- [Gestion des identités et des accès dans Amazon S3 Glacier](#) dans le Manuel du développeur S3 Glacier.
- [Comment créer la stratégie de cycle de vie d'un compartiment S3 ? \(p. 83\)](#)
- [Comment restaurer un objet S3 supprimé ? \(p. 50\)](#)

## Comment verrouiller un objet Amazon S3 ?

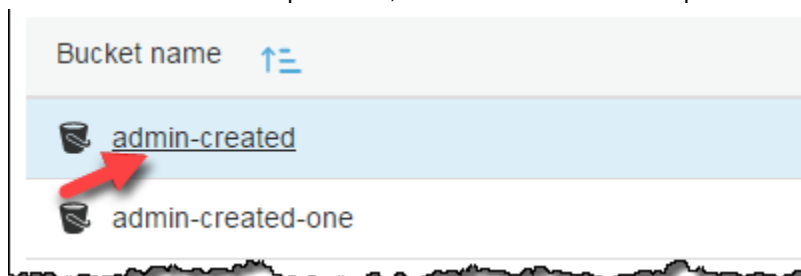
S3 Verrouillage d'objet vous permet de stocker des objets dans Amazon S3 selon un modèle « Write Once Read Many » (WORM). En utilisant S3 Verrouillage d'objet, vous pouvez empêcher qu'un objet ne soit supprimé ou remplacé sur une période déterminée ou indéfinie. Pour de plus amples informations sur le verrouillage d'objets à l'aide de l'AWS CLI, des kits SDK AWS et des API REST Amazon S3, veuillez consulter [Verrouillage d'objets à l'aide de Verrouillage d'objet](#) dans le Amazon Simple Storage Service Manuel du développeur.

Avant de verrouiller des objets, vous devez activer un compartiment pour utiliser S3 Verrouillage d'objet. Vous activez Verrouillage d'objet lorsque vous créez un compartiment. Une fois que vous avez activé Verrouillage d'objet sur un compartiment, vous pouvez verrouiller les objets de ce dernier. Après avoir créé un compartiment dans lequel Verrouillage d'objet est activé, vous ne pouvez pas désactiver Verrouillage d'objet ou interrompre la gestion des versions pour ce compartiment.

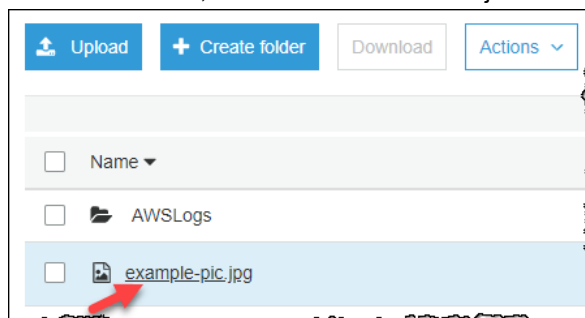
Pour de plus amples informations sur la création d'un compartiment avec S3 Verrouillage d'objet activé, veuillez consulter [Comment créer un compartiment S3 ? \(p. 4\)](#).

Pour verrouiller un objet Amazon S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.



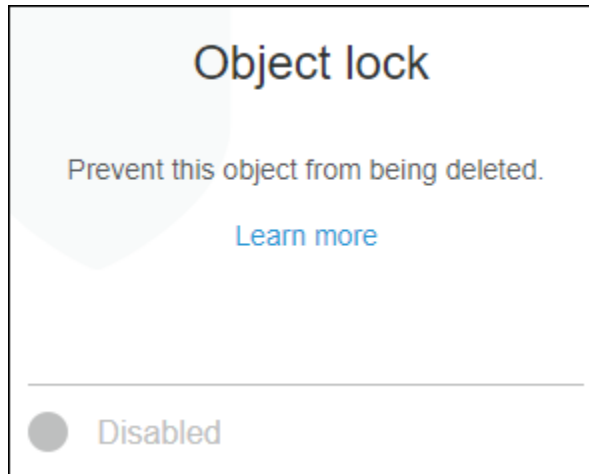
3. Dans la liste Nom, choisissez le nom de l'objet à verrouiller.



4. Choisissez Propriétés.



5. Choisissez Verrouillage d'objet.



6. Choisissez un mode de rétention. Vous pouvez modifier la date figurant dans le champ Retain until date (Conserver jusqu'au). Vous pouvez également choisir d'activer une mise en suspens juridique. Pour de plus amples informations, veuillez consulter [Présentation de S3 Verrouillage d'objet](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Object lock

Prevent objects from being deleted in order to help ensure data integrity and regulatory compliance. [Learn more](#)

**Retention mode**

☒ **Enable governance mode**  
Governance mode can be disabled by AWS accounts that have specific IAM permissions.

☐ **Enable compliance mode**  
Compliance mode cannot be disabled by any user, including the root account.

☐ **Disable**

**Retain until date**

2018-11-27

**Legal hold**  
Legal hold prevents an object from being deleted regardless of its retain until date. Legal hold can be applied and removed by AWS accounts that have specific IAM permissions.

☐ **Enable**

☒ **Disable**

[Cancel](#) [Save](#)

7. Choisissez Enregistrer.

## Plus d'informations

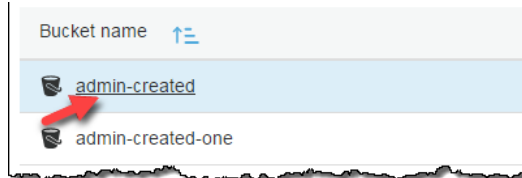
- [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#)

## Comment afficher la présentation d'un objet ?

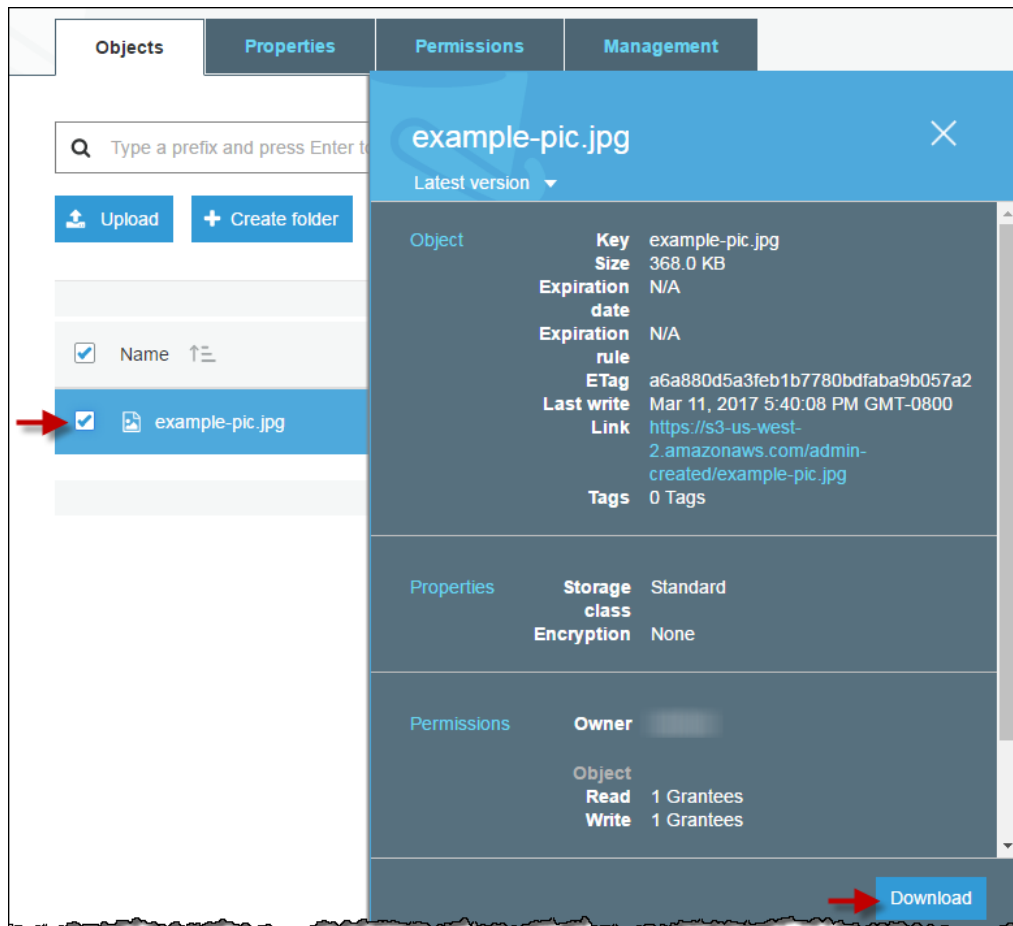
Cette section explique comment utiliser la console Amazon S3 pour afficher le panneau de présentation d'un objet. Ce panneau de présentation affiche en un même endroit toutes les informations essentielles pour un objet.

Pour afficher le panneau de présentation d'un objet

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.



3. Dans la liste Nom, cochez la case en regard du nom de l'objet dont vous souhaitez afficher la présentation.



4. Pour télécharger l'objet, choisissez Télécharger dans le panneau de présentation de l'objet. Pour copier le chemin de l'objet dans le presse-papiers, choisissez Chemin de copie.





5. Si la gestion des versions est activée pour le compartiment, choisissez **Dernières versions** pour afficher la liste de toutes les versions de l'objet. Vous pouvez ensuite choisir l'icône de téléchargement pour télécharger la version d'un objet ou l'icône de corbeille pour la supprimer.



### Important

Vous pouvez annuler la suppression d'un objet uniquement si celui-ci a été supprimé en tant que version la plus récente (version actuelle). Vous ne pouvez pas restaurer une version précédente d'un objet supprimé. Pour plus d'informations, consultez [Gestion des versions d'un objet](#) et [Utilisation de la gestion des versions](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Plus d'informations

- [Comment afficher les versions d'un objet S3 ? \(p. 61\)](#)

## Comment afficher les versions d'un objet S3 ?

Cette section explique comment utiliser la console Amazon S3 pour afficher les différentes versions d'un objet.

Un compartiment pour lequel la gestion des versions est activée peut comporter de nombreuses versions d'un même objet : une version actuelle (la plus récente), et aucune, une ou plusieurs versions anciennes (précédentes). Amazon S3 attribue un ID de version unique à chaque objet. Pour plus d'informations sur l'activation de la gestion des versions, consultez [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#).

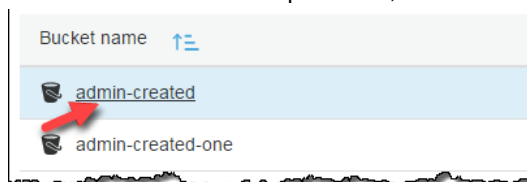
Si la gestion des versions est activée pour un compartiment, Amazon S3 crée une autre version d'un objet dans les cas suivants :

- Si vous chargez un objet dont le nom est identique à celui d'un objet qui existe déjà dans le compartiment, Amazon S3 crée une autre version de l'objet au lieu de remplacer l'objet existant.
- Si vous mettez à jour les propriétés de l'objet après avoir chargé celui-ci dans le compartiment, comme le changement des détails de stockage ou tout autre changement de métadonnées, Amazon S3 crée une nouvelle version d'objet dans le compartiment.

Pour plus d'informations sur la prise en charge de la gestion des versions dans Amazon S3, consultez [Gestion des versions d'un objet](#) et [Utilisation de la gestion des versions](#) dans le Amazon Simple Storage Service Manuel du développeur.

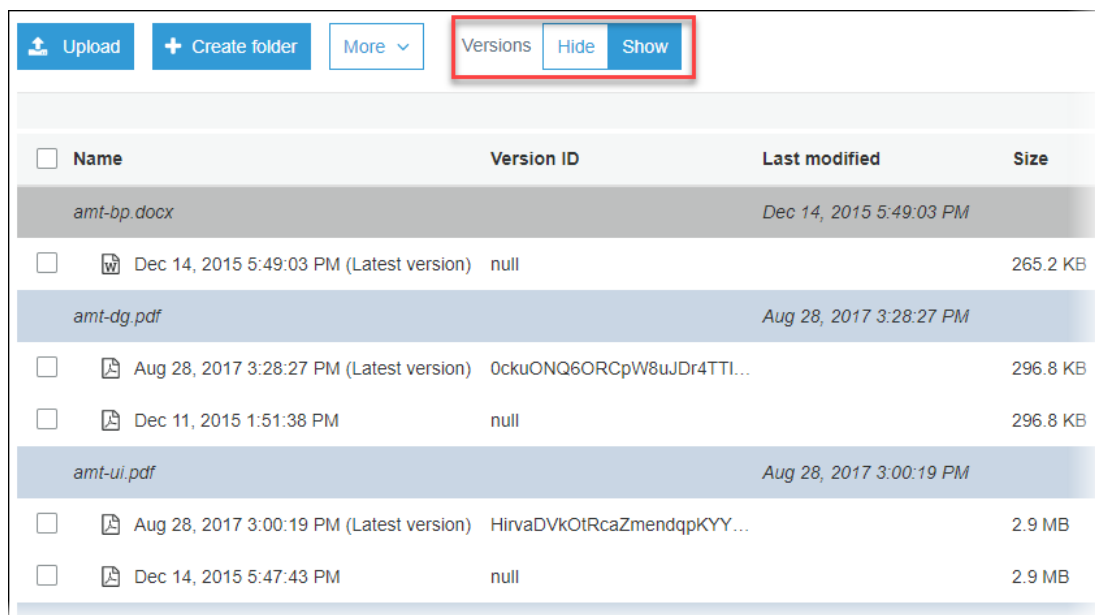
Pour afficher différentes versions d'un objet






1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.



3. Pour accéder à une liste des versions d'un objet du compartiment, choisissez Afficher. Pour chaque version d'objet, la console affiche un ID de version unique, la date et l'heure auxquelles la version d'objet a été créée, et d'autres propriétés. (Les objets stockés dans le compartiment avant la configuration de l'état de la gestion des versions possèdent un ID de version null.)

Pour afficher la liste des objets sans les versions, choisissez Masquer.



<input type="checkbox"/>	Name	Version ID	Last modified	Size
<input type="checkbox"/>	amt-bp.docx		Dec 14, 2015 5:49:03 PM	
<input type="checkbox"/>	 Dec 14, 2015 5:49:03 PM (Latest version)	null		265.2 KB
<input type="checkbox"/>	amt-dg.pdf		Aug 28, 2017 3:28:27 PM	
<input type="checkbox"/>	 Aug 28, 2017 3:28:27 PM (Latest version)	0ckuONQ6ORCpW8uJDr4TTI...		296.8 KB
<input type="checkbox"/>	 Dec 11, 2015 1:51:38 PM	null		296.8 KB
<input type="checkbox"/>	amt-ui.pdf		Aug 28, 2017 3:00:19 PM	
<input type="checkbox"/>	 Aug 28, 2017 3:00:19 PM (Latest version)	HirvaDVkOtRcaZmendqpKYY...		2.9 MB
<input type="checkbox"/>	 Dec 14, 2015 5:47:43 PM	null		2.9 MB

Vous pouvez également afficher, télécharger et supprimer les versions d'un objet dans le panneau de présentation de l'objet. Pour plus d'informations, consultez [Comment afficher la présentation d'un objet ? \(p. 58\)](#).

#### Important

Vous pouvez annuler la suppression d'un objet uniquement si celui-ci a été supprimé en tant que version la plus récente (version actuelle). Vous ne pouvez pas restaurer une version précédente d'un objet supprimé. Pour plus d'informations, consultez [Gestion des versions d'un objet](#) et [Utilisation de la gestion des versions](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Plus d'informations

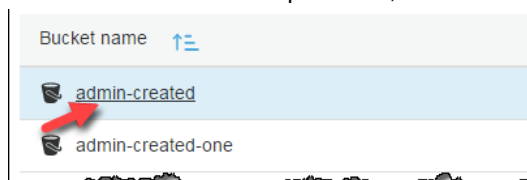
- [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#)
- [Comment créer la stratégie de cycle de vie d'un compartiment S3 ? \(p. 83\)](#)

## Comment afficher les propriétés d'un objet ?

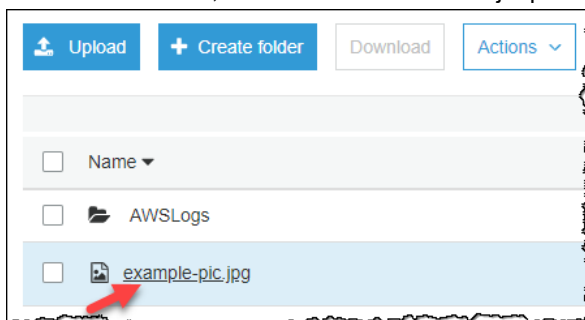
Cette section explique comment utiliser la console pour afficher les propriétés d'un objet.

Pour afficher les propriétés d'un objet

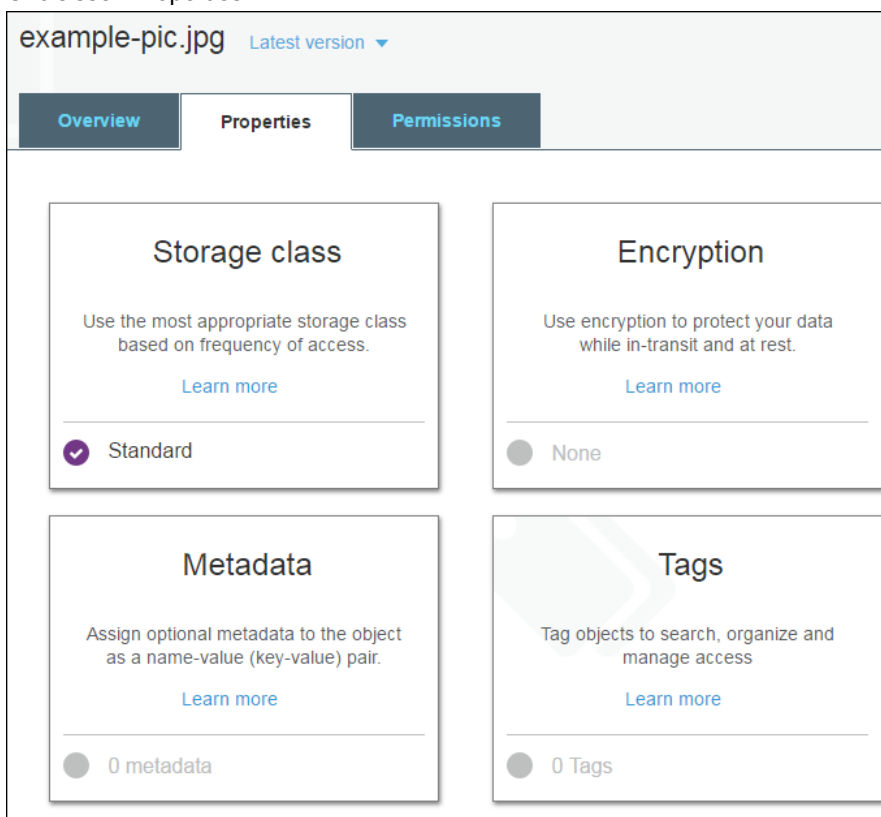
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.



3. Dans la liste Name, choisissez le nom de l'objet pour lequel vous souhaitez afficher les propriétés.



4. Choisissez Properties.



5. Sur la page Propriétés, vous pouvez configurer les propriétés suivantes pour l'objet.

#### Note

Si vous modifiez les propriétés Storage Class, Encryption et Metadata, un nouvel objet est créé pour remplacer l'ancien. Si l'option Gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

- a. Classe de stockage – Chaque objet dans Amazon S3 possède une classe de stockage qui lui est associée. La classe de stockage que vous choisissez d'utiliser dépend de la fréquence à laquelle vous accédez à l'objet. La classe de stockage par défaut pour les objets S3 est STANDARD. Vous choisissez la classe de stockage à utiliser lors du chargement d'un objet. Pour plus d'informations sur les classes de stockage, consultez [Classes de stockage](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour modifier la classe de stockage après le chargement d'un objet, choisissez Classe de stockage. Choisissez la classe de stockage de votre choix, puis cliquez sur Enregistrer.

- b. Chiffrement – Vous pouvez chiffrer vos objets S3. Pour plus d'informations, consultez [Comment ajouter le chiffrement à un objet S3 ? \(p. 64\)](#).
- c. Métadonnées – Chaque objet dans Amazon S3 possède un ensemble de paires nom-valeur qui représente ses métadonnées. Pour plus d'informations sur l'ajout de métadonnées à un objet S3, consultez [Comment ajouter des métadonnées à un objet S3 ? \(p. 67\)](#).
- d. Balises – Vous pouvez ajouter des balises à un objet S3. Pour plus d'informations, consultez [Comment ajouter des balises à un objet S3 ? \(p. 73\)](#).

## Comment ajouter le chiffrement à un objet S3 ?

Cette rubrique décrit comment définir ou modifier le type de chiffrement qu'un objet utilise à l'aide de la console Amazon S3.

### Note

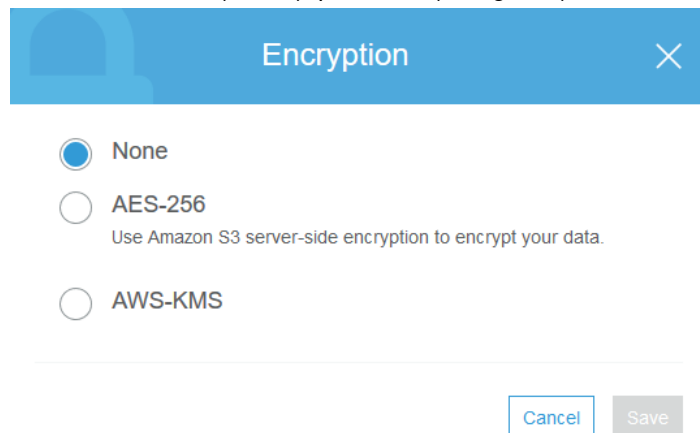
Si vous modifiez le chiffrement d'un objet, un nouvel objet est créé pour remplacer l'ancien. Si l'option Gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

Pour ajouter ou modifier le chiffrement d'un objet

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.
3. Dans la liste Name (Nom), choisissez le nom de l'objet pour lequel vous souhaitez ajouter ou modifier le chiffrement.
4. Choisissez Propriétés, puis Chiffrement.

La boîte de dialogue Chiffrement qui s'ouvre propose trois options pour le chiffrement des objets :

- Aucun- Aucun chiffrement d'objet.
  - AES-256 - Chiffrement côté serveur avec clés gérées par Amazon S3 (SSE-S3).
  - AWS-KMS - Chiffrement côté serveur avec clés principales client AWS Key Management Service (AWS KMS) (SSE-KMS).
5. Si vous souhaitez supprimer le chiffrement d'un objet possédant déjà des paramètres de chiffrement, sélectionnez None (Aucun), puis Save (Enregistrer).



Encryption

☒ None

☐ AES-256  
Use Amazon S3 server-side encryption to encrypt your data.

☐ AWS-KMS

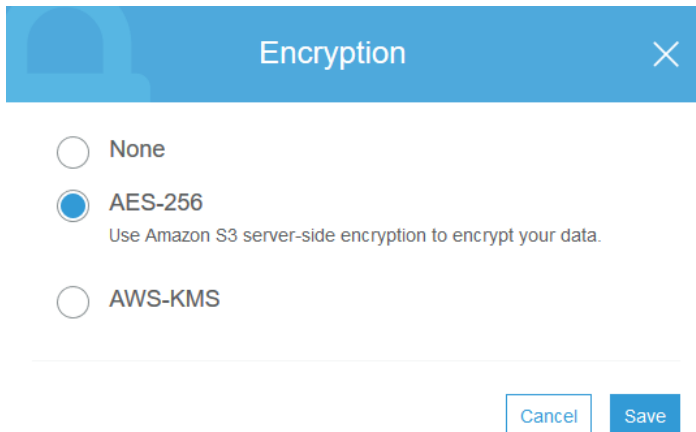
Cancel Save

6. Si vous souhaitez chiffrer votre objet à l'aide de clés gérées par Amazon S3, procédez comme suit :

- a. Sélectionnez AES-256.

Pour plus d'informations sur l'utilisation du chiffrement côté serveur d'Amazon S3, consultez [Protection des données avec des clés de chiffrement gérées par Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

- b. Choisissez Enregistrer.



7. Si vous souhaitez chiffrer votre objet à l'aide d' AWS KMS, procédez comme suit :

- a. Choisissez AWS-KMS.


- b. Choisissez une clé CMK AWS KMS.

La liste indique les [clés CMK gérées par le client](#) que vous avez créées ainsi que votre clé CMK gérée par AWS pour Amazon S3. Pour plus d'informations sur la création de clés CMK AWS KMS gérées par le client, consultez [Création de clés](#) dans le AWS Key Management Service Developer Guide.

#### Important

La console Amazon S3 répertorie uniquement 100 clés CMK AWS KMS par région AWS. Si vous avez plus de 100 clés CMK dans la même région, vous ne pouvez voir que les 100 premières CMK dans la console S3. Pour utiliser une clé CMK KMS qui n'est pas répertoriée dans la console, choisissez ARN KMS personnalisé, puis saisissez l'ARN CMK KMS.

- c. Choisissez Enregistrer.



Encryption

☐ None

☐ AES-256  
Use Amazon S3 server-side encryption to encrypt your data.

☒ AWS-KMS

example-key

Cancel


Save

### Important

Pour chiffrer des objets dans le compartiment, vous pouvez uniquement utiliser les clés CMK qui sont activées dans la même région AWS que le compartiment. Amazon S3 ne prend en charge que les clés CMK symétriques. Amazon S3 ne prend pas en charge les clés CMK asymétriques. Pour plus d'informations, consultez les informations relatives à l'[utilisation des clés symétriques et asymétriques](#).

8. Pour permettre à un compte externe d'utiliser un objet protégé par une clé CMK AWS KMS, procédez comme suit :
  - a. Choisissez AWS-KMS.
  - b. Saisissez l'Amazon Resource Name (ARN) du compte externe.
  - c. Choisissez Enregistrer.

Les administrateurs d'un compte externe qui disposent des autorisations d'utilisation sur un objet protégé par votre clé CMK AWS KMS peuvent ensuite restreindre l'accès en créant une stratégie AWS Identity and Access Management (IAM) au niveau des ressources.



Encryption

☐ None

☐ AES-256  
Use Amazon S3 server-side encryption to encrypt your data.

☒ AWS-KMS

Custom KMS ARN

Cancel

Save

#### Note

Cette action applique le chiffrement à tous les objets spécifiés. Lors du chiffrement de dossiers, attendez la fin de l'opération d'enregistrement pour ajouter de nouveaux objets au dossier.

## Plus d'informations

- [Comment activer le chiffrement par défaut pour un compartiment Amazon S3 ? \(p. 9\)](#)
- [Chiffrement par défaut d'Amazon S3 pour compartiments S3](#) dans le Amazon Simple Storage Service Manuel du développeur
- [Comment afficher les propriétés d'un objet ? \(p. 62\)](#)
- [Chargement, téléchargement et gestion d'objets \(p. 36\)](#)

## Comment ajouter des métadonnées à un objet S3 ?

Chaque objet dans Amazon Simple Storage Service (Amazon S3) possède un ensemble de paires nom-valeur qui fournissent des métadonnées sur l'objet. Les métadonnées sont des informations supplémentaires sur l'objet. Certaines métadonnées sont définies par Amazon S3 lorsque vous chargez l'objet, par exemple, `Date` et `Content-Length`. Vous pouvez également définir certaines métadonnées lorsque vous chargez l'objet ou les ajouter ultérieurement. Cette section explique comment utiliser la console Amazon S3 pour ajouter des métadonnées à un objet S3.

Les métadonnées d'objet sont un ensemble de paires nom-valeur (clé-valeur). Par exemple, les métadonnées de longueur du contenu, `Content-Length`, indiquent le nom (clé) et la taille de l'objet en octets (valeur). Pour plus d'informations sur les métadonnées d'objet, consultez [Métadonnées d'objet](#) dans le Amazon Simple Storage Service Manuel du développeur.

Il existe deux types de métadonnées pour un objet S3, les métadonnées définies par le système Amazon S3 et celles définies par l'utilisateur :

- **Métadonnées système** – Il existe deux classes de métadonnées système. Les métadonnées telles que la date `Last-Modified` sont contrôlées par le système. Seul Amazon S3 peut modifier la valeur. Il existe également des métadonnées système que vous contrôlez, par exemple la classe de stockage configurée pour l'objet.
- **Métadonnées définies par l'utilisateur** – Vous pouvez définir vos propres métadonnées personnalisées, appelées métadonnées définies par l'utilisateur. Vous pouvez affecter des données définies par l'utilisateur à un objet lorsque vous le chargez ou après son chargement. Les métadonnées définies par l'utilisateur sont stockées avec l'objet et renvoyées lorsque vous téléchargez l'objet. Amazon S3 ne traite pas les métadonnées définies par l'utilisateur.

Les rubriques suivantes expliquent comment ajouter des métadonnées à un objet à l'aide de la console Amazon S3.

#### Note

Si vous modifiez les métadonnées d'un objet, un nouvel objet sera créé et remplacera l'ancien. Si l'option Gestion des versions S3 est activée, une nouvelle version de l'objet est créée et l'objet existant devient une version plus ancienne. Le rôle qui modifie la propriété devient également le propriétaire du nouvel objet ou (version de l'objet).

#### Rubriques

- [Ajout de métadonnées définies par le système à un objet S3 \(p. 68\)](#)
- [Ajout de métadonnées définies par l'utilisateur à un objet S3 \(p. 70\)](#)



## Ajout de métadonnées définies par le système à un objet S3

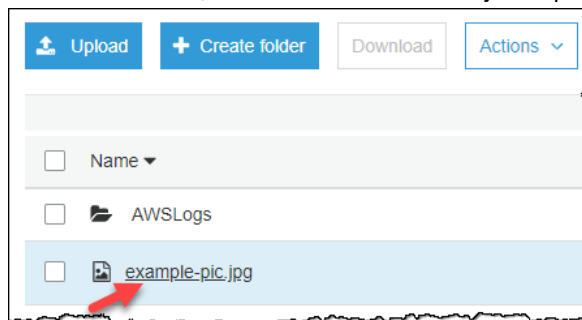
Vous pouvez configurer certaines données système pour un objet S3. Pour obtenir la liste des métadonnées définies par le système et pour savoir si vous pouvez modifier leur valeur, consultez [Métadonnées définies par le système](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour ajouter des métadonnées système à un objet

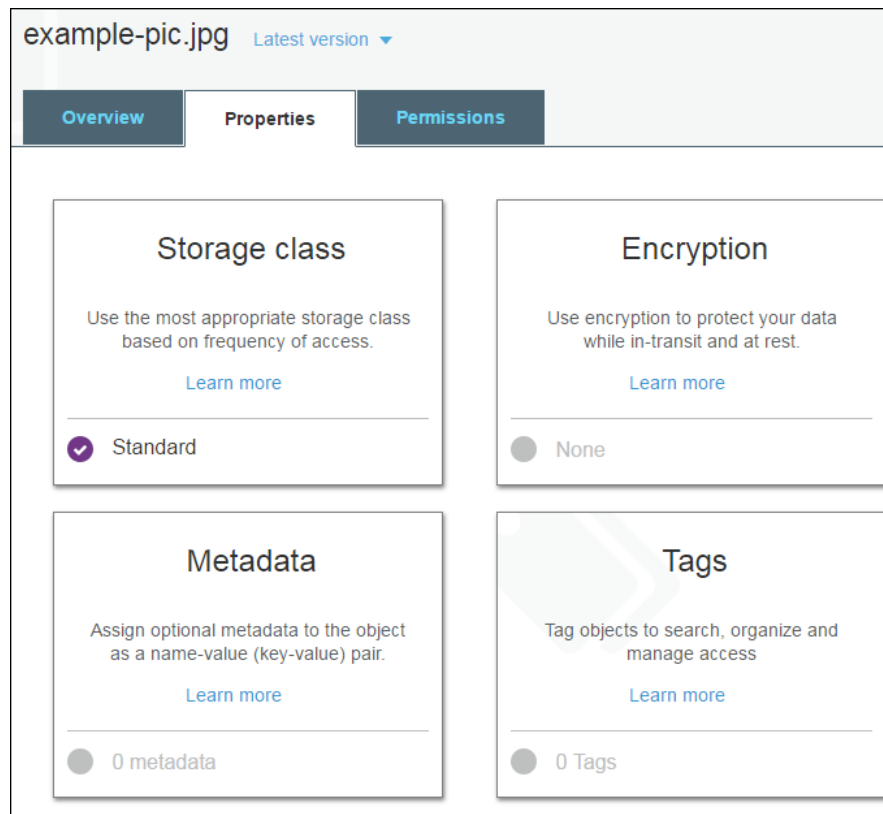
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.



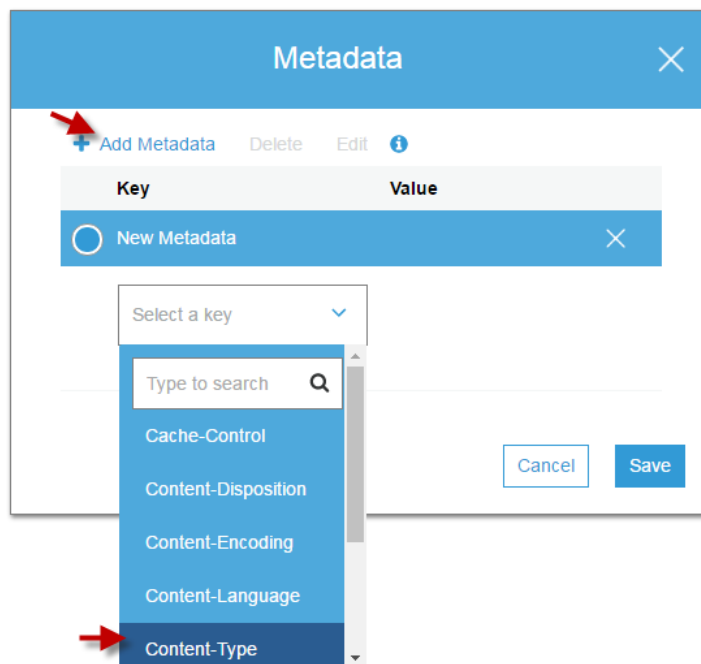
3. Dans la liste Nom, choisissez le nom de l'objet auquel vous voulez ajouter des métadonnées.



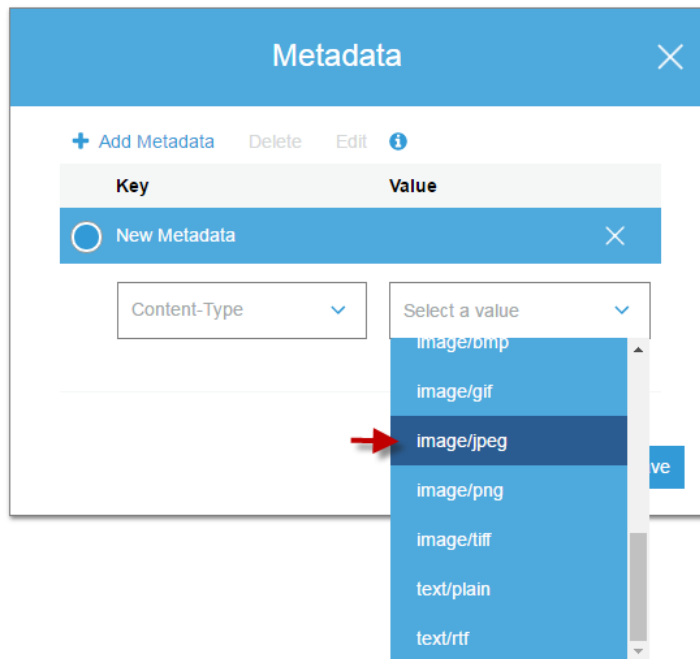
4. Choisissez Propriétés, puis Métadonnées.



5. Choisissez Ajouter les métadonnées, puis sélectionnez une clé dans le menu Sélectionner une clé.



6. Selon la clé choisie, choisissez une valeur dans le menu Sélectionner une valeur ou saisissez une valeur.

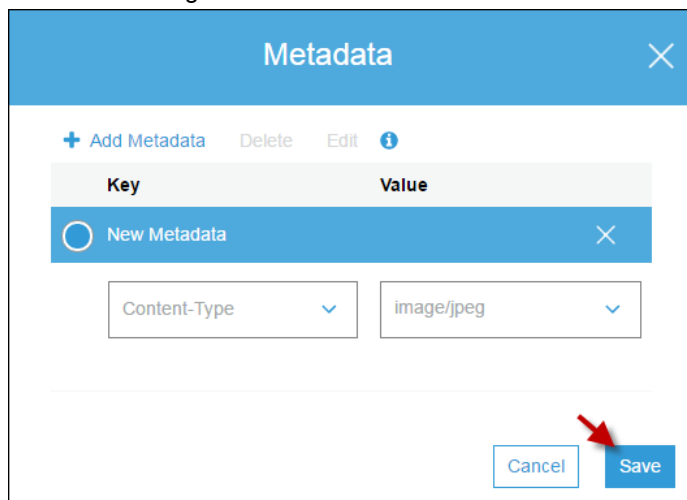


The screenshot shows the 'Metadata' dialog box with a table for adding metadata. The 'Key' column has 'Content-Type' selected. The 'Value' column has a dropdown menu open, showing a list of MIME types. A red arrow points to 'image/jpeg' in the list.

Key	Value
Content-Type	Select a value

- image/bmp
- image/gif
- image/jpeg
- image/png
- image/tiff
- text/plain
- text/rtf

7. Choisissez Enregistrer.



The screenshot shows the 'Metadata' dialog box with the 'Value' dropdown menu now displaying 'image/jpeg'. A red arrow points to the 'Save' button at the bottom right of the dialog.

Key	Value
Content-Type	image/jpeg

Cancel Save

#### Note

Cette action ajoute des métadonnées à tous les objets spécifiés. Lors de l'ajout de métadonnées à des dossiers, attendez la fin de l'opération d'enregistrement pour ajouter de nouveaux objets au dossier.

## Ajout de métadonnées définies par l'utilisateur à un objet S3

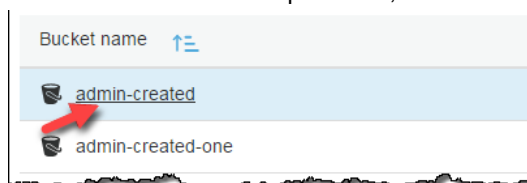
Vous pouvez affecter des métadonnées définies par l'utilisateur à un objet. Les métadonnées définies par l'utilisateur doivent commencer par le préfixe « x-amz-meta- », sinon Amazon S3 ne configure pas la paire clé-valeur comme vous l'avez définie. Pour définir des métadonnées personnalisées, vous

devez ajouter le nom de votre choix à la clé `x-amz-meta-`. Cette action crée une clé personnalisée. Par exemple, si vous ajoutez le nom personnalisé `alt-name`, la clé de métadonnées est `x-amz-meta-alt-name`.

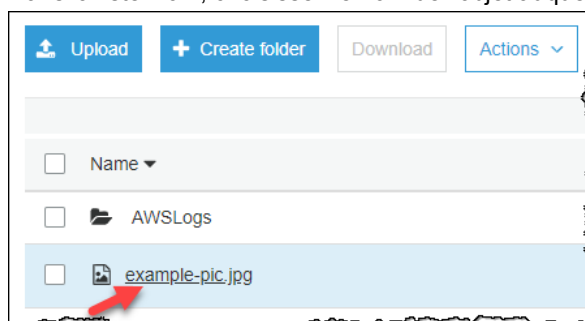
Les métadonnées définies par l'utilisateur peuvent atteindre 2 Ko. Les clés et leurs valeurs doivent respecter les normes US-ASCII. Pour plus d'informations, consultez [Métadonnées définies par l'utilisateur](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour ajouter des métadonnées définies par l'utilisateur à un objet

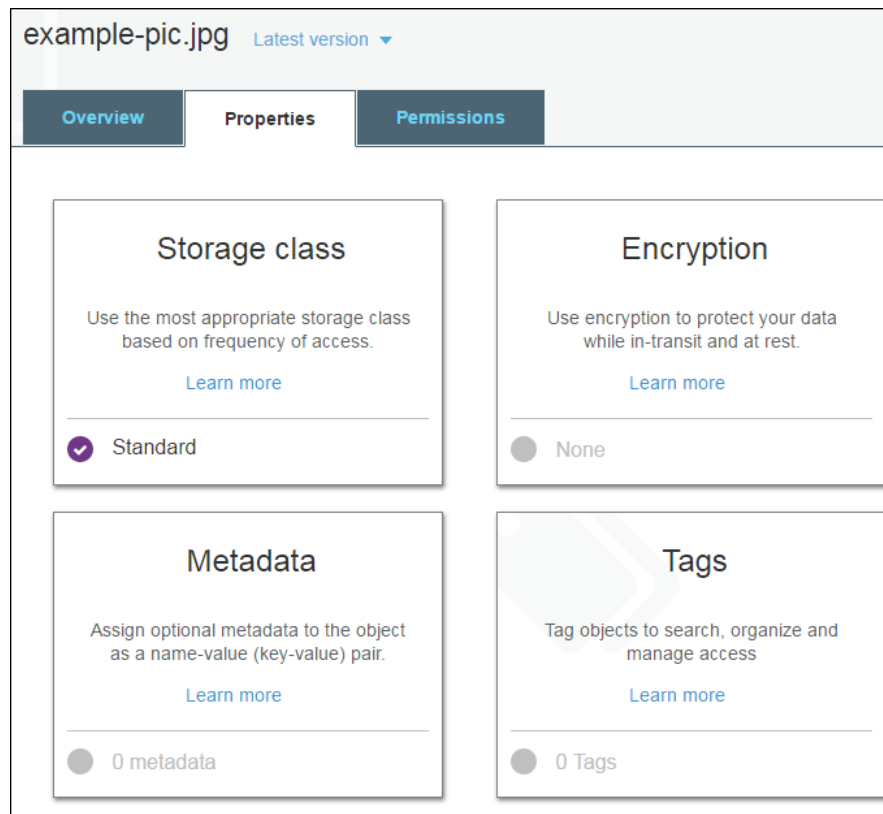
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.



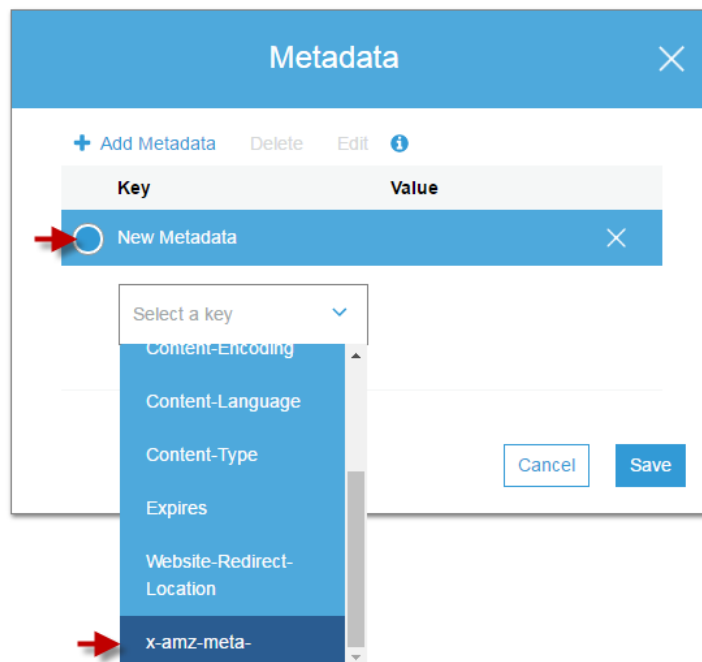
3. Dans la liste Nom, choisissez le nom de l'objet auquel vous voulez ajouter des métadonnées.



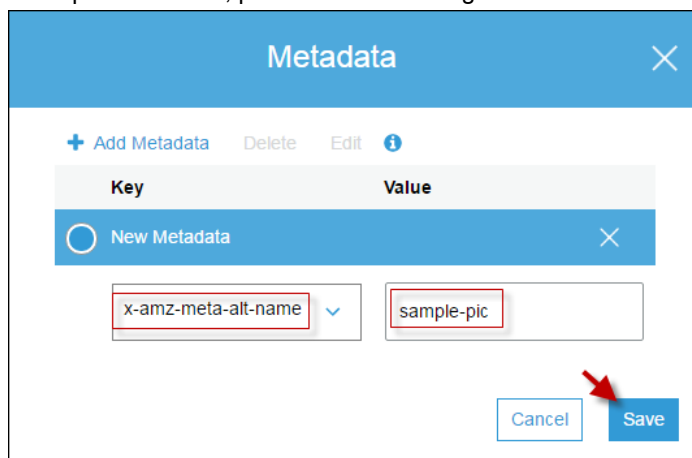
4. Choisissez Propriétés, puis Métadonnées.



5. Choisissez Ajouter des métadonnées, puis sélectionnez la clé `x-amz-meta-` dans le menu Sélectionner une clé. Toute métadonnée commençant par le préfixe `x-amz-meta-` est une métadonnée définie par l'utilisateur.



6. Saisissez un nom personnalisé à la suite de la clé `x-amz-meta-`. Par exemple, pour le nom personnalisé `alt-name`, la clé de métadonnées est `x-amz-meta-alt-name`. Entrez une valeur pour la clé personnalisée, puis choisissez Enregistrer.



#### Note

Lors de l'ajout de métadonnées à des dossiers, attendez la fin de l'enregistrement pour ajouter de nouveaux objets. Dans le cas contraire, de nouveaux objets pourraient également être modifiés.

## Plus d'informations

- [Comment afficher les propriétés d'un objet ? \(p. 62\)](#)
- [Chargement, téléchargement et gestion d'objets \(p. 36\)](#)

## Comment ajouter des balises à un objet S3 ?

Le balisage des objets vous permet de classer le stockage par catégorie. Cette rubrique explique comment utiliser la console pour ajouter des balises à un objet S3 une fois que ce dernier a été chargé. Pour plus d'informations sur l'ajout de balises à un objet après son chargement, consultez [Comment charger des fichiers ou des dossiers dans un compartiment S3 ? \(p. 37\)](#).

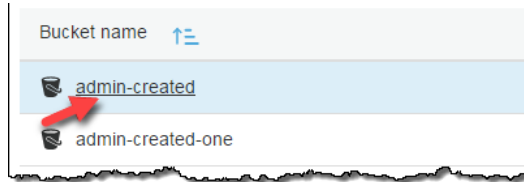
Chaque balise est une paire clé-valeur qui respecte les règles suivantes :

- Vous pouvez associer jusqu'à 10 balises à un objet. Les balises associées à un objet doivent avoir des clés de balise uniques.
- Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 255 caractères Unicode.
- Les valeurs de clés et de balises sont sensibles à la casse.

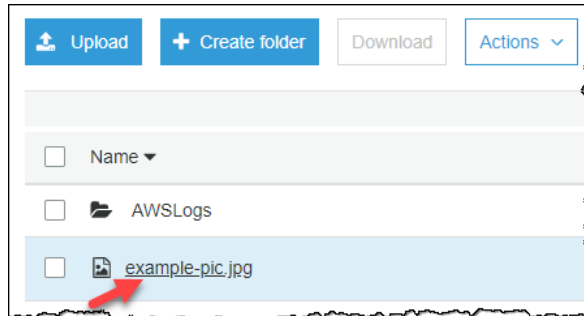
Pour plus d'informations sur les balises d'objets, consultez [Balisage des objets](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour ajouter des balises à un objet

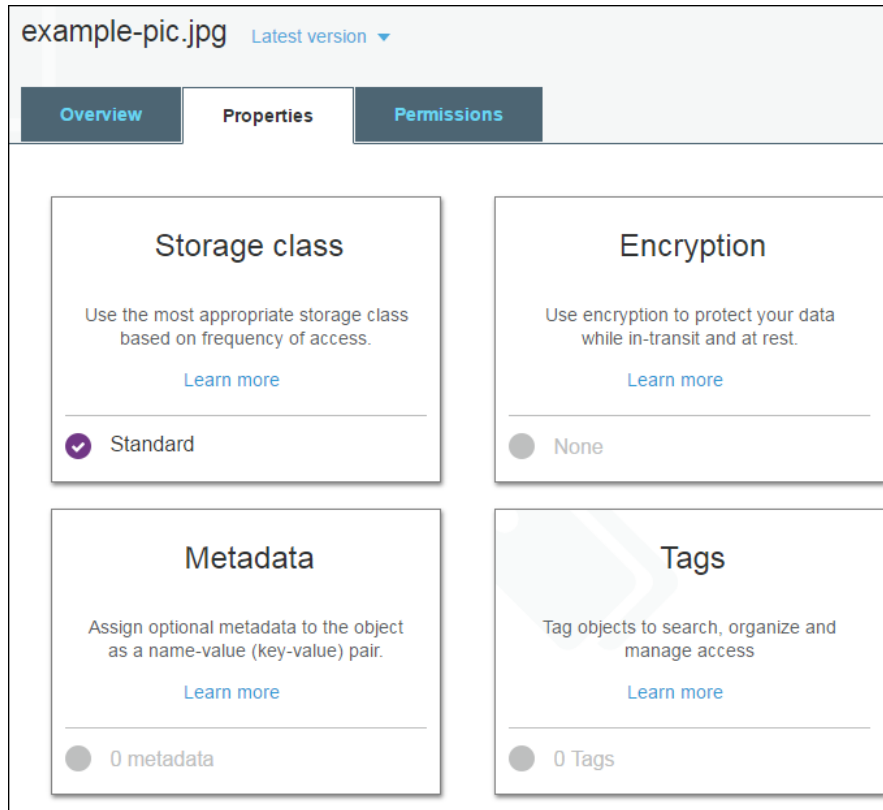
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.



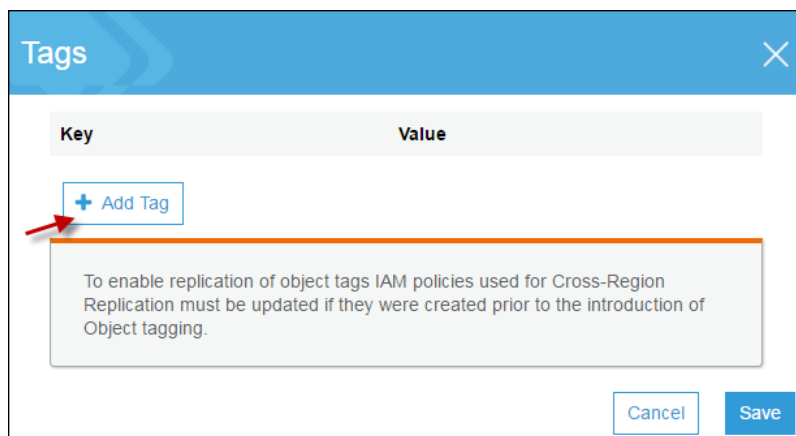
3. Dans la liste Nom, choisissez le nom de l'objet auquel vous voulez ajouter des balises.



4. Choisissez Properties.

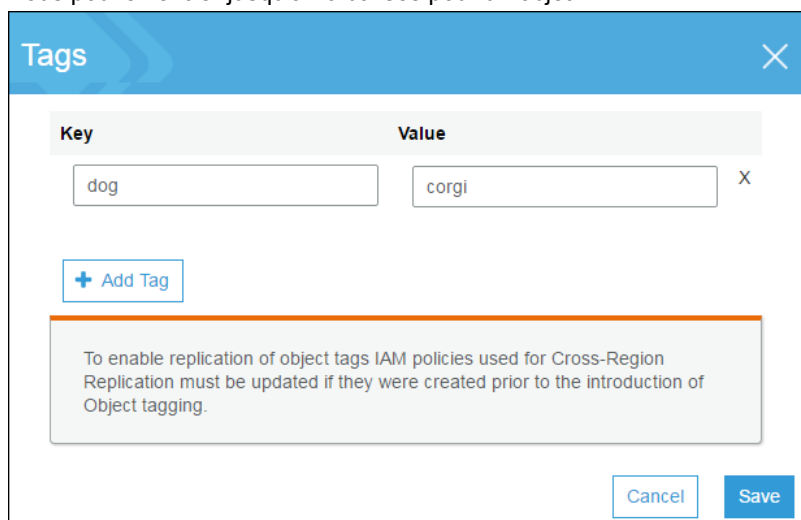


5. Choisissez Balises, puis Ajouter une balise.



6. Chaque balise est une paire clés-valeurs. Saisissez des éléments dans les champs Key et Value. Choisissez ensuite Add Tag pour ajouter une autre balise ou choisissez Save.

Vous pouvez entrer jusqu'à 10 balises pour un objet.



## Plus d'informations

- [Comment afficher les propriétés d'un objet ? \(p. 62\)](#)
- [Chargement, téléchargement et gestion d'objets \(p. 36\)](#)

## Comment utiliser les dossiers d'un compartiment S3 ?

Dans Amazon S3, les compartiments et les objets sont les ressources principales, et les objets sont stockés dans des compartiments. Amazon S3 possède une structure horizontale et non une hiérarchie que vous pourriez voir dans un système de fichiers. Toutefois, par souci de simplification organisationnelle, la console Amazon S3 prend en charge le concept du dossier comme moyen de regrouper des objets. Amazon S3 y parvient en utilisant un préfixe de nom partagé pour les objets (c'est-à-dire, les objets dont les noms commencent par une chaîne commune). Les noms d'objet sont également appelés noms de clé.



Par exemple, vous pouvez créer un dossier dans la console appelé `photos` et y stocker un objet nommé `myphoto.jpg`. L'objet est ensuite stocké avec le nom de clé `photos/myphoto.jpg`, dans lequel le préfixe est `photos/`.

Voici deux exemples supplémentaires :

- Si vous possédez trois objets dans le compartiment : `—logs/date1.txt`, `logs/date2.txt` et `logs/date3.txt`—, la console affiche un dossier appelé `logs`. Si vous ouvrez le dossier dans la console, vous voyez les trois objets : `date1.txt`, `date2.txt` et `date3.txt`.
- Si vous avez un objet appelé `photos/2017/example.jpg`, la console affiche un dossier appelé `photos` qui contient le dossier `2017` et l'objet `example.jpg`.

#### Rubriques

- [Création d'un dossier \(p. 76\)](#)
- [Comment supprimer des dossiers d'un compartiment S3 ? \(p. 78\)](#)
- [Rendre les dossiers publics \(p. 80\)](#)

Vous pouvez avoir des dossiers dans d'autres dossiers, mais pas de compartiments dans d'autres compartiments. Vous pouvez charger et copier des objets directement dans un dossier. Des dossiers peuvent être créés, supprimés et rendus publics, mais ils ne peuvent pas être renommés. Des objets peuvent être copiés d'un dossier vers un autre.

#### Important

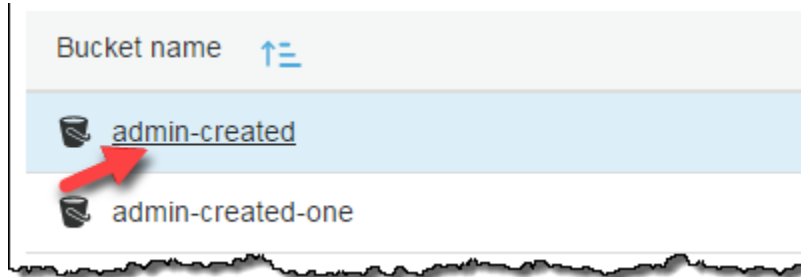
- La console Amazon S3 implémente la création d'objets de dossier en créant un objet de type zéro octet avec la valeur de préfixe et délimiteur du dossier comme clé. Ces objets de dossier n'apparaissent pas dans la console, mais se comportent comme n'importe quel autre objet ; ils peuvent être consultés et manipulés via l'API, l'interface de ligne de commande AWS et les kits SDK.
- La console Amazon S3 traite tous les objets, dont le nom de clé possède une barre oblique « / » à la fin, comme des dossiers, par exemple `examplekeyname/`. Vous ne pouvez pas charger un objet qui possède un nom de clé avec une « / » à la fin à l'aide de la console Amazon S3. Toutefois, vous pouvez charger les objets dont le nom se termine par une « / » avec l'API Amazon S3 grâce à l'AWS CLI, les kits SDK AWS ou l'API REST.
- Un objet dont le nom se termine par une « / » apparaît en tant que dossier dans la console Amazon S3. La console Amazon S3 n'affiche pas le contenu et les métadonnées pour un tel objet. Lorsque vous utilisez la console pour copier un objet dont le nom se termine par une « / », un nouveau dossier est créé dans l'emplacement de destination mais les données et métadonnées de l'objet ne sont pas copiées.

## Création d'un dossier

Cette section décrit comment utiliser la console Amazon S3 pour créer un dossier.

#### Pour créer un dossier

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment dans lequel vous souhaitez créer un dossier.



3. Choisissez Créer un dossier.



4. Attribuez un nom au dossier (par exemple, **favorite-pics**). Choisissez le paramètre de chiffrement pour l'objet de dossier, puis choisissez Enregistrer.

A screenshot of the Amazon S3 console showing the 'Create folder' dialog box. The folder name 'favorite-pics' is entered in the text field. Below the text field, there is a message: 'When you create a folder, S3 console creates an object with the above name appended by suffix "/" and that object is displayed as a folder in the S3 console. Choose the encryption setting for the object:'. There are three radio button options: 'None (Use bucket settings)' (selected), 'AES-256' (with subtext 'Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)'), and 'AWS-KMS' (with subtext 'Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)'). At the bottom, there are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted.

5. Si vous ne souhaitez pas utiliser le chiffrement avec votre dossier, choisissez None (Aucun).
6. Si vous souhaitez chiffrer votre objet à l'aide de clés gérées par Amazon S3, procédez comme suit :
- Choisissez AES-256.

Pour de plus amples informations sur l'utilisation du chiffrement côté serveur Amazon S3, veuillez consulter [Protection des données avec des classes des clés de chiffrement gérées par Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

7. Si vous souhaitez chiffrer votre objet à l'aide d' AWS KMS, procédez comme suit :
- a. Choisissez AWS-KMS.
  - b. Choisissez une clé CMK AWS KMS.

La liste indique les [clés CMK gérées par le client](#) que vous avez créées ainsi que votre clé CMK gérée par AWS pour Amazon S3. Pour plus d'informations sur la création de clés CMK AWS KMS gérées par le client, consultez [Création de clés](#) dans le AWS Key Management Service Developer Guide.

### Important

Pour chiffrer des objets dans le compartiment, vous pouvez uniquement utiliser les clés CMK qui sont activées dans la même région AWS que le compartiment. Amazon S3 ne prend en charge que les clés CMK symétriques et ne prend pas en charge les clés CMK asymétriques. Pour de plus amples informations, veuillez consulter [Utilisation des clés symétriques et asymétriques](#).

La console Amazon S3 ne répertorie que 100 clés CMK KMS par région. Si vous avez plus de 100 clés CMK dans la même région, vous ne pouvez voir que les 100 premières CMK dans la console S3. Pour utiliser une clé CMK AWS KMS qui n'est pas répertoriée dans la console, choisissez Custom KMS ARN (ARN KMS personnalisé), puis saisissez l'ARN CMK KMS.

8. Choisissez Enregistrer.

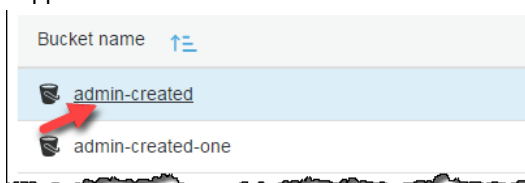
## Comment supprimer des dossiers d'un compartiment S3 ?

Cette section explique comment utiliser la console Amazon S3 pour supprimer des dossiers d'un compartiment S3.

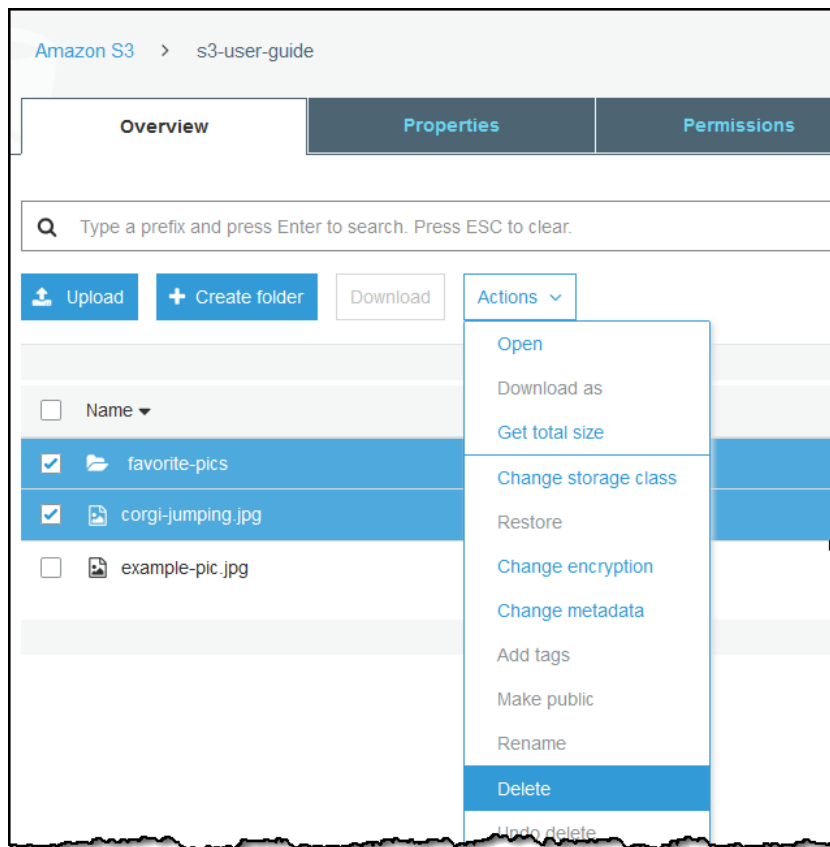
Pour plus d'informations sur les fonctionnalités et la tarification d'Amazon S3, consultez [Amazon S3](#).

Pour supprimer des dossiers d'un compartiment S3

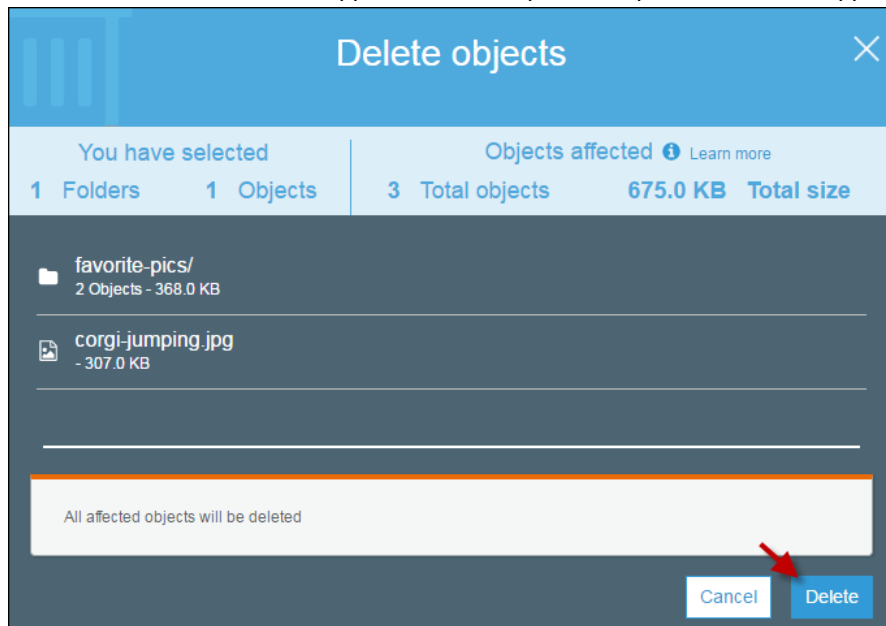
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment à partir duquel vous souhaitez supprimer des dossiers.



3. Dans la liste Nom, cochez la case en regard des dossiers et des objets à supprimer, choisissez More, puis Supprimer.



Dans la boîte de dialogue Supprimer les objets, vérifiez que les noms des dossiers que vous avez sélectionnés en vue de leur suppression sont répertoriés, puis choisissez Supprimer.



#### Warning

Cette action supprime tous les objets spécifiés. Lorsque vous supprimez des dossiers, attendez la fin de l'action de suppression pour ajouter de nouveaux objets au dossier. Dans le cas contraire, de nouveaux objets pourraient également être supprimés.

## Voir aussi

- [Comment supprimer des objets d'un compartiment S3 ? \(p. 49\)](#)

## Rendre les dossiers publics

Amazon S3 possède une structure horizontale et non une hiérarchie que vous pourriez voir habituellement dans un système de fichiers. Toutefois, par souci de simplification organisationnelle, la console Amazon S3 prend en charge le concept du dossier comme moyen de regrouper des objets. Dans Amazon S3, le dossier est un préfixe de dénomination pour un objet ou un groupe d'objets. Pour de plus amples informations, veuillez consulter [Comment utiliser les dossiers d'un compartiment S3 ? \(p. 75\)](#)

Nous vous recommandons de bloquer tout l'accès public à vos dossiers et compartiments Amazon S3, à moins que vous ayez besoin spécifiquement d'un dossier ou compartiment public. Lorsque vous rendez public un dossier, quiconque sur Internet peut voir tous les objets qui sont regroupés dans ce dossier. Dans la console Amazon S3, vous pouvez rendre public un dossier. Vous pouvez également rendre public un dossier en créant une stratégie de compartiment qui limite l'accès par préfixe. Pour plus d'informations, consultez [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#).

#### Warning

Une fois que vous avez rendu public un dossier dans la console Amazon S3, vous ne pouvez pas le rendre à nouveau privé. Au lieu de cela, vous devez définir des autorisations sur chaque objet individuel dans le dossier public de sorte que les objets n'aient pas d'accès public. Pour de plus amples informations, veuillez consulter [Comment définir les autorisations d'un objet ? \(p. 124\)](#)

## Plus d'informations

- [Comment supprimer des dossiers d'un compartiment S3 ? \(p. 78\)](#)
- [Comment définir des autorisations de compartiment ACL ? \(p. 127\)](#)
- [Comment bloquer l'accès public à des compartiments S3 ? \(p. 119\)](#)

# Présentation de Opérations par lot S3.

Les Opérations par lot S3 exécutent des opérations par lot à grande échelle sur les objets Amazon S3. Vous pouvez utiliser les Opérations par lot S3 pour copier des objets, définir des balises d'objet ou des listes de contrôle d'accès (ACL), lancer des restaurations d'objets à partir de Amazon S3 Glacier ou appeler une fonction AWS Lambda afin d'effectuer des actions personnalisées en utilisant vos objets. Vous pouvez effectuer ces opérations sur une liste personnalisée d'objets ou utiliser un rapport d'inventaire Amazon S3 pour faciliter la génération de listes d'objets, même les plus volumineuses. Les Opérations par lot S3 utilisent les mêmes API Amazon S3 que celles que vous utilisez déjà, ce qui signifie que vous connaissez déjà l'interface. Pour de plus amples informations sur l'exécution de Opérations par lot S3 à l'aide du AWS CLI, des kits AWS SDK et des API REST Amazon S3, veuillez consulter [Exécution de Opérations par lot S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

Les rubriques suivantes expliquent comment utiliser la console Amazon S3 pour configurer et exécuter des opérations par lot.

## Rubriques

- [Création d'une tâche Opérations par lot S3 \(p. 81\)](#)
- [Gestion des tâches Opérations par lot S3 \(p. 82\)](#)

## Création d'une tâche Opérations par lot S3

Cette section décrit comment créer une tâche Opérations par lot S3. Pour de plus amples informations sur l'exécution de Opérations par lot à l'aide du AWS CLI, des kits AWS SDK et des API REST Amazon S3, veuillez consulter [Exécution de Opérations par lot S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

### Pour créer un travail par lot

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez dans Opérations par lot le volet de navigation de la console Amazon S3.
3. Choisissez Create job (Créer un travail).
4. Choisissez la région dans laquelle vous souhaitez créer le travail.
5. Sous Format du manifeste, choisissez le type d'objet manifeste à utiliser.
  - Si vous choisissez S3 Inventory report (Rapport d'inventaire S3), entrez le chemin vers l'objet manifest.json généré par Amazon S3 dans le cadre du rapport d'inventaire au format CSV et, éventuellement, l'ID de version de l'objet manifeste si vous souhaitez utiliser une version autre que la version la plus récente.
  - Si vous choisissez CSV, entrez le chemin vers un objet manifeste au format CSV. L'objet manifeste doit respecter le format décrit dans la console. Vous pouvez éventuellement inclure l'ID de version de l'objet manifeste si vous souhaitez utiliser une version autre que la plus récente.
6. Choisissez Suivant.
7. Sous Opération, choisissez l'opération que vous souhaitez effectuer sur tous les objets listés dans le manifeste. Remplissez les informations relatives à l'opération choisie, puis sélectionnez Suivant.

8. Remplissez les informations relatives à l'option Configure additional options (Configurer les options supplémentaires), puis sélectionnez Suivant.
9. Sous Vérification, vérifiez les paramètres. Si vous devez apporter des modifications, choisissez Précédent. Sinon, choisissez Create Job (Créer le travail).

## Plus d'informations

- [Les bases : tâches Opérations par lot S3](#) dans le Amazon Simple Storage Service Manuel du développeur
- [Création d'une tâche Opérations par lot S3](#) dans le Amazon Simple Storage Service Manuel du développeur
- [Opérations](#) dans le Amazon Simple Storage Service Manuel du développeur

## Gestion des tâches Opérations par lot S3

Amazon S3 fournit un ensemble d'outils pour vous aider à gérer vos tâches d'Opérations par lot S3 après les avoir créées. Pour de plus amples informations sur la gestion de Opérations par lot S3, veuillez consulter [Gestion des tâches Opérations par lot S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Plus d'informations

- [Les bases : tâches Opérations par lot S3](#) dans le Amazon Simple Storage Service Manuel du développeur
- [Création d'une tâche Opérations par lot S3](#) dans le Amazon Simple Storage Service Manuel du développeur
- [Opérations](#) dans le Amazon Simple Storage Service Manuel du développeur

# Gestion du stockage

Cette section explique comment configurer les outils de gestion de stockage d'Amazon S3.

## Rubriques

- [Comment créer la stratégie de cycle de vie d'un compartiment S3 ? \(p. 83\)](#)
- [Comment ajouter une règle de réplication à un compartiment S3 ? \(p. 87\)](#)
- [Comment gérer les règles de réplication pour un compartiment S3 ? \(p. 103\)](#)
- [Comment configurer une analyse de classe de stockage ? \(p. 105\)](#)
- [Comment configurer l'inventaire Amazon S3 ? \(p. 109\)](#)
- [Comment créer un filtre de métriques des demandes pour tous les objets de mon compartiment S3 ? \(p. 114\)](#)
- [Comment créer un filtre de métriques des demandes qui limite la portée par balise ou préfixe d'objet ? \(p. 115\)](#)
- [Comment supprimer un filtre de métriques des demandes ? \(p. 116\)](#)
- [Comment afficher les métriques de réplication ? \(p. 117\)](#)

## Comment créer la stratégie de cycle de vie d'un compartiment S3 ?

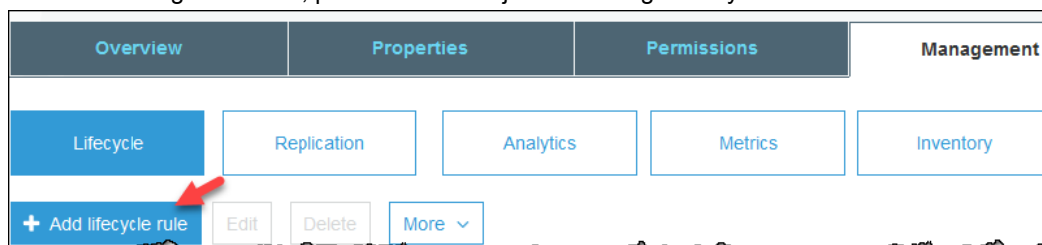
Vous pouvez utiliser des stratégies de cycle de vie pour définir les actions qu'Amazon S3 doit effectuer au cours de la durée de vie d'un objet (par exemple, transférer les objets vers une autre classe de stockage, les archiver ou les supprimer au bout d'un certain laps de temps).

Vous pouvez définir une stratégie de cycle de vie pour tous les objets ou pour un sous-ensemble d'objets du compartiment à l'aide d'un préfixe partagé (c'est-à-dire des objets dont le nom commence par une chaîne commune) ou d'une balise.

Une stratégie de cycle de vie vous permet de définir des actions propres aux versions d'objets actuelles et anciennes. Pour plus d'informations, consultez [Gestion du cycle de vie des objets](#), [Gestion des versions d'un objet](#) et [Utilisation de la gestion des versions](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Pour créer une stratégie de cycle de vie

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Compartiments, choisissez le nom du compartiment pour lequel vous souhaitez créer une stratégie de cycle de vie.
3. Choisissez l'onglet Gestion, puis choisissez Ajouter une règle de cycle de vie.

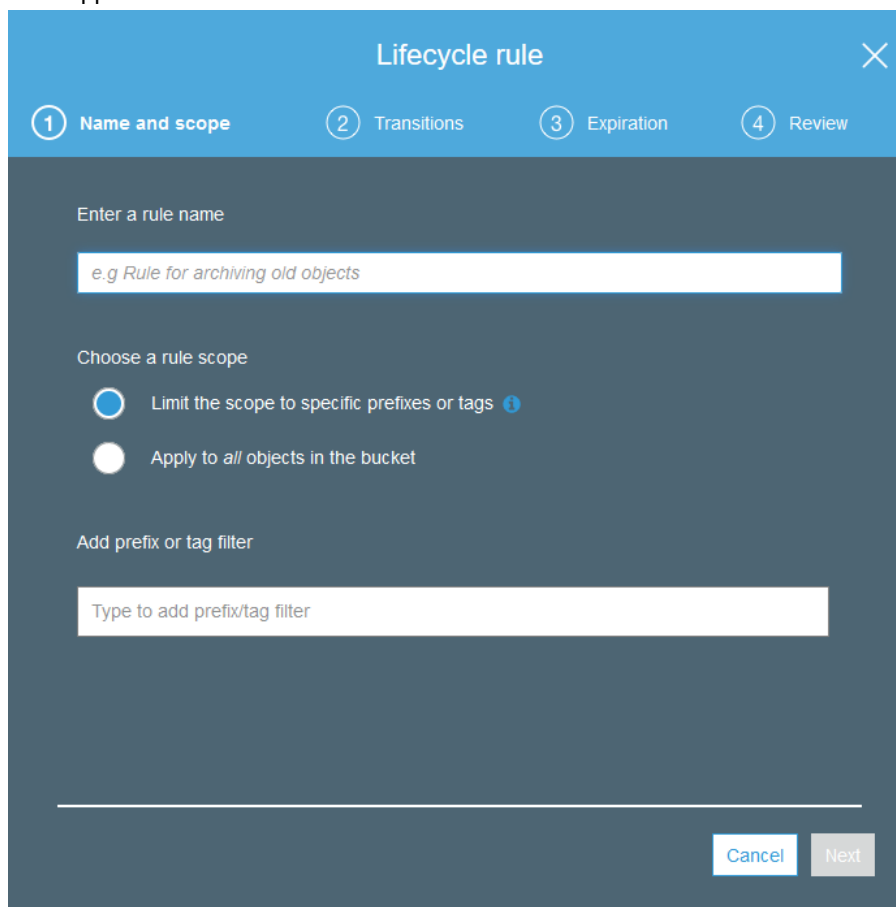




4. Dans la boîte de dialogue Règle de cycle de vie, tapez un nom pour votre règle.

Ce nom doit être unique dans le compartiment.

5. Choisissez la portée de la règle de cycle de vie : tous les objets avec un préfixe ou une balise spécifique ou tous les objets du compartiment.
  - Pour appliquer cette règle de cycle de vie à tous les objets avec un préfixe ou une balise spécifique, choisissez Limiter la portée à des préfixes ou balises spécifiques. Dans la zone Ajouter un préfixe ou un filtre de balises, tapez le préfixe ou le nom de la balise, puis appuyez sur Saisir. Pour plus d'informations sur les préfixes de nom d'objet, consultez [Clés d'objet](#) dans le Amazon Simple Storage Service Manuel du développeur. Pour plus d'informations sur les balises d'objet, reportez-vous à la section [Balisage des objets](#) dans le Amazon Simple Storage Service Manuel du développeur.



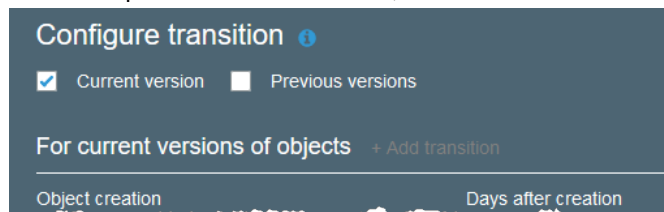
- Pour appliquer cette règle de cycle de vie à tous les objets du compartiment, choisissez Appliquer à tous les objets du compartiment.
6. Choisissez Suivant.

La page Transition de classe de stockage s'ouvre. Lorsque vous configurez les transitions de vos classes de stockage, vous définissez les règles de transition des objets vers les classes de stockage Standard - Accès peu fréquent, Unizone - Accès peu fréquent, Glacier et Deep Archive. Pour de plus amples informations, veuillez consulter [Classes de stockage](#) dans le manuel Amazon Simple Storage Service Manuel du développeur. Vous pouvez définir le transfert des versions actuelles ou précédentes des objets, ou des deux versions à la fois. La gestion des versions vous permet de conserver plusieurs versions d'un objet au sein d'un même compartiment. Pour plus d'informations sur la gestion des versions, consultez [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ?](#) (p. 8).

7. Choisissez les versions pour lesquelles vous souhaitez définir des transitions, actuelles ou non :

- Sélectionnez Version actuelle pour définir les transferts qui s'appliquent à la version actuelle de l'objet.
- Sélectionnez Versions précédentes pour définir les transitions qui s'appliquent à toutes les versions précédentes de l'objet.

Dans la capture d'écran ci-dessous, Version actuelle est choisie.

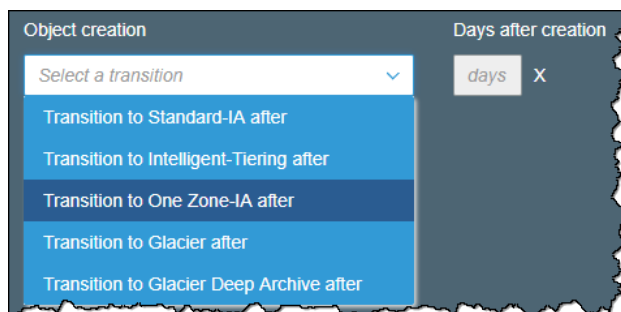


8. Pour ajouter une transition :

- a. Pour une version actuelle, sous For current object versions (Pour les versions d'objet actuelles), choisissez Ajouter une transition.
- b. Pour une version non actuelle, sous For non-current object versions (Pour les versions d'objet non actuelles), choisissez Ajouter une transition.

9. Pour chaque transition que vous ajoutez, choisissez l'une des options suivantes :

- Transition vers Standard - Accès peu fréquent après.
- Transition vers Intelligent-Tiering (Hiérarchisation intelligente) après.
- Transition vers Unizone - Accès peu fréquent après.
- Transition vers Glacier après.
- Transition vers Glacier Deep Archive après.



### Important

Lorsque vous choisissez les classes de stockage Glacier ou Glacier Deep Archive, vos objets restent dans Amazon S3. Vous ne pouvez pas y accéder directement via le service Amazon S3 Glacier séparé. Pour plus d'informations, consultez [Transition d'objets utilisant le cycle de vie Amazon S3](#).

10. Dans la zone Jours après la création, entrez combien de jours après la création de l'objet vous souhaitez appliquer la transition (par exemple, 30 ou 100 jours).
11. Lorsque vous avez terminé de configurer les transferts, choisissez Suivant.

**Lifecycle rule**

1 Name and scope 2 **Transitions** 3 Expiration 4 Review

### Storage class transition

You can add rules in a lifecycle configuration to tell Amazon S3 to transition objects to another storage class. There are **per-request fees** when using lifecycle to transition data to any S3 or S3 Glacier storage class. [Learn more](#) or see [Amazon S3 pricing](#)

☒ Current version ☒ Previous versions

**For current versions of objects** + Add transition

Object creation	Days after creation
Transition to Standard-IA after	30 X

**For previous versions of objects** + Add transition

Object becomes a previous version	Days after objects become noncurrent
Transition to Glacier Deep Archive after	100 X

[Previous](#) [Next](#)

12. Sous Configurer l'expiration, dans cet exemple, choisissez Version actuelle et Versions précédentes.

#### Important

Dans un compartiment non activé pour la gestion des versions, l'action d'expiration a pour résultat la suppression permanente de l'objet dans Amazon S3. Pour de plus amples informations sur les actions du cycle de vie, veuillez consulter [Éléments pour décrire les actions du cycle de vie](#) dans le Amazon Simple Storage Service Manuel du développeur.

13. Sélectionnez Faire expirer la version actuelle de l'objet, puis indiquez le délai (en nombre de jours) au terme duquel supprimer l'objet (395 jours, par exemple).

Si vous sélectionnez cette option d'expiration, vous ne pouvez pas sélectionner l'option de nettoyage des marqueurs de suppression expirés.

14. Sélectionnez Supprimer définitivement les versions précédentes, puis indiquez le délai (en nombre de jours) au terme duquel un objet devient une version précédente en vue de le supprimer définitivement (465 jours, par exemple).
15. Pour nettoyer les chargements partitionnés non terminés, nous vous recommandons de choisir Nettoyer les chargements partitionnés non terminés et de saisir combien de jours après le début du chargements partitionnés vous souhaitez terminer et nettoyer les chargements partitionnés non terminés (par exemple, 7 jours).

Pour plus d'informations sur les téléchargements partitionnés, consultez [Présentation du téléchargement partitionné](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

16. Choisissez Suivant.

**Lifecycle rule**

✓ Name and scope   ✓ Transitions   **3 Expiration**   4 Review

**Configure expiration**

☒ Current version   ☒ Previous versions

☒ Expire current version of object ⓘ

After  days from object creation

☒ Permanently delete previous versions ⓘ

After  days from becoming a previous version

**Clean up expired object delete markers and incomplete multipart uploads**

☐ Clean up expired object delete markers ⓘ

You cannot enable clean up expired object delete markers if you enable Expiration.

☒ Clean up incomplete multipart uploads ⓘ

After  Days from start of upload

[Previous](#) [Next](#)

17. Sous Révision, vérifiez les paramètres de votre règle. Si vous devez apporter des modifications, choisissez Précédent. Sinon, choisissez Save.

Si la règle ne contient aucune erreur, elle est activée et vous pouvez la voir sur la page Cycle de vie.

<a href="#">+ Add lifecycle rule</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">More ▾</a>
Lifecycle rule	Applied to	Actions for current version	Actions for previous version(s)
testrule	Whole bucket	Standard-IA / Expire	Standard-IA / Amazon Glacier / Permanently Delete

## Comment ajouter une règle de réplication à un compartiment S3 ?

La réplication est une fonctionnalité qui permet la copie d'objets automatique et asynchrone entre les compartiments de différentes régions AWS ou d'une même région AWS. Elle réplique les objets nouvellement créés et les mises à jour d'objets d'un compartiment source vers un compartiment de destination. Pour de plus amples informations sur les concepts de la réplication et sur l'utilisation de la réplication avec l'interface de ligne de commande AWS, les kits SDK AWS et les API REST Amazon S3, veuillez consulter [Réplication](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour pouvoir utiliser la réplication, la gestion des versions doit être activée sur les compartiments source et de destination. Pour connaître la liste complète des exigences, veuillez consulter [Exigences pour la réplication](#) dans le Amazon Simple Storage Service Manuel du développeur. Pour plus d'informations

sur la gestion des versions, consultez [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#)

Les répliques d'objets du compartiment de destination sont des répliques exactes des objets du compartiment source. Ils ont les mêmes noms de clé et les mêmes métadonnées, par exemple l'heure de création, le propriétaire, les métadonnées définies par l'utilisateur, l'ID de version, la liste de contrôle d'accès (ACL) et la classe de stockage. Vous avez également la possibilité de spécifier explicitement une classe de stockage différente pour les répliques d'objet. Et quel que soit le propriétaire du compartiment ou de l'objet source, vous pouvez choisir de remplacer le propriétaire des répliques par le compte AWS qui possède le compartiment de destination. Pour de plus amples informations, veuillez consulter [Modification du propriétaire d'un réplica](#) dans le Amazon Simple Storage Service Manuel du développeur.

Vous pouvez utiliser S3 Replication Time Control (S3 RTC) pour répliquer vos données dans la même région AWS ou dans différentes régions AWS dans un délai prévisible. S3 RTC réplique 99,99 % des nouveaux objets stockés dans Amazon S3 dans les 15 minutes et la plupart des objets en quelques secondes. Pour plus d'informations, consultez [Replicating Objects Using S3 Replication Time Control \(S3 RTC\)](#) dans le Amazon Simple Storage Service Manuel du développeur.

#### Remarque sur les règles de réplication et de cycle de vie

Les métadonnées restent identiques entre l'objet d'origine et la réplique de l'objet. Les règles de cycle de vie respectent l'heure de création de l'objet d'origine, et non celle à laquelle l'objet répliqué devient disponible dans le compartiment de destination. Toutefois, le cycle de vie n'agit pas sur les objets en attente de réplication tant que la réplication n'est pas terminée.

Utilisez la console Amazon S3 pour ajouter des règles de réplication dans le compartiment source. Les règles de réplication définissent les objets du compartiment source à répliquer, ainsi que le compartiment de destination dans lequel les objets répliqués seront stockés. Vous pouvez créer une règle pour répliquer tous les objets ou un sous-ensemble d'objets d'un compartiment à l'aide de préfixes de nom de clé ou d'autres balises d'objet, ou les deux. Un compartiment de destination peut se trouver dans le même compte AWS que le compartiment source, mais il peut également se trouver dans un autre compte.

Si vous spécifiez un ID de version d'objet à supprimer, Amazon S3 supprime cette version de l'objet dans le compartiment source. Mais le service ne réplique pas la suppression dans le compartiment de destination. En d'autres termes, il ne supprime pas la même version de l'objet dans le compartiment de destination. Les données sont ainsi protégées contre les suppressions malencontreuses.

Si le compartiment de destination se trouve dans un compte différent du compartiment source, vous devez ajouter une stratégie de compartiment au compartiment de destination pour accorder au propriétaire du compte du compartiment source l'autorisation d'effectuer des répliques d'objets dans le compartiment de destination. La console Amazon S3 construit la stratégie de compartiment requise pour que vous puissiez copier et ajouter le compartiment de destination dans l'autre compte.

Lorsque vous ajoutez une règle de réplication à un compartiment, celle-ci est activée par défaut et entre en fonctionnement dès que vous l'enregistrez.

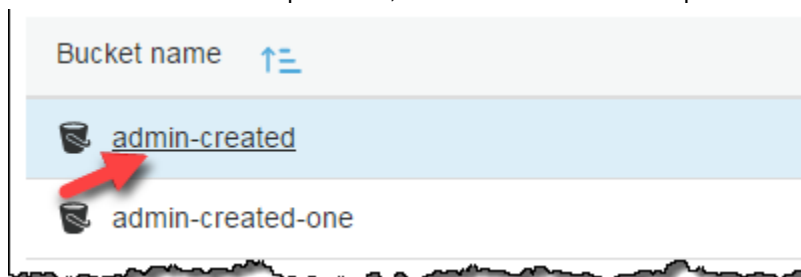
#### Rubriques

- [Ajout d'une règle de réplication lorsque le compartiment de destination est dans le même compte AWS \(p. 89\)](#)
- [Ajout d'une règle de réplication lorsque le compartiment de destination est dans un compte AWS distinct \(p. 96\)](#)
- [Plus d'informations \(p. 103\)](#)

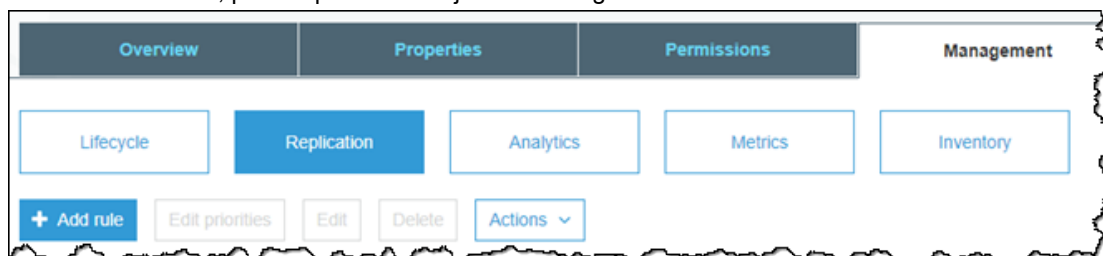
## Ajout d'une règle de réplication lorsque le compartiment de destination est dans le même compte AWS

Suivez ces étapes pour configurer une règle de réplication quand le compartiment de destination se trouve dans le même compte AWS que le compartiment source.

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.



3. Choisissez Gestion, puis Réplication et Ajouter une règle.



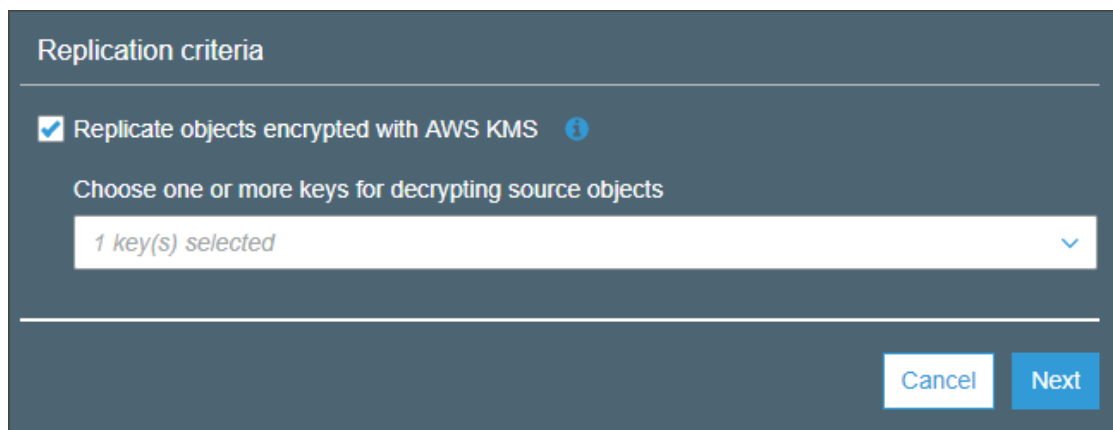
4. Dans l'Assistant Règle de réplication, sous Définir la source, vous avez les options suivantes pour définir la source de réplication :
  - Pour répliquer la totalité du compartiment, choisissez Totalité du compartiment **nom-compartiment**.
  - Pour répliquer tous les objets avec le même préfixe (par exemple, tous les objets dont le nom commence par la chaîne `pictures`), choisissez Préfixe ou balises. Entrez un préfixe dans la zone, choisissez le préfixe dans la liste déroulante et appuyez sur Entrée. Si vous entrez un préfixe correspondant à un nom de dossier, vous devez insérer le caractère / (barre oblique) à la fin (par exemple, `pictures/`). Pour plus d'informations sur les préfixes, consultez [Création de clés](#) dans le Amazon Simple Storage Service Manuel du développeur.
  - Pour répliquer tous les objets ayant une ou plusieurs balises d'objet, tapez une balise dans la zone, choisissez la balise dans la liste déroulante, puis appuyez sur Entrée. Entrez la valeur de la balise et appuyez sur Entrée. Répétez la procédure pour ajouter une autre balise. Vous pouvez combiner un préfixe et des balises. Pour plus d'informations sur les balises d'objets, consultez [Balisage des objets](#) dans le Amazon Simple Storage Service Manuel du développeur.

The screenshot shows the 'Replication rule' configuration window in the AWS Management Console. The window has a blue header with the title 'Replication rule' and a close button (X). Below the header is a progress bar with four steps: 1. Set source (active), 2. Set destination, 3. Configure options, and 4. Review. The 'Set source' section is expanded, showing two radio button options: 'Entire bucket' (with a bucket icon) and 'Prefix or tags' (with an information icon). The 'Prefix or tags' option is selected. Below these options are two text input fields: 'Type to add prefix/tag filter' and 'Type in a prefix name or tag key name'.

Le nouveau schéma prend en charge le balisage de préfixe et de balise, et la priorité des règles. Pour de plus amples informations sur le nouveau schéma, consultez [Rétrocompatibilité de la configuration de réplication](#) dans le Amazon Simple Storage Service Manuel du développeur. Le guide du développeur décrit le XML utilisé avec l'API Amazon S3 qui fonctionne derrière l'interface utilisateur. Dans le guide du développeur, le nouveau schéma est décrit comme configuration de réplication XML V2.

5. Pour répliquer des objets du compartiment source qui sont chiffrés avec AWS Key Management Service (AWS KMS), sous Replication criteria (Critères de réplication), sélectionnez Replicate objects encrypted with AWS KMS (Répliquer les objets chiffrés avec KMS). Sous Choose one or more keys for decrypting source objects (Choisir une ou plusieurs clés de déchiffrement des objets de la source) figurent la ou les clés CMK AWS KMS source que vous autorisez la réplication à utiliser. Toutes les clés CMK source sont incluses par défaut. Vous pouvez choisir d'affiner la sélection des clés CMK.

Les objets chiffrés par les clés CMK AWS KMS que vous ne sélectionnez pas ne sont pas répliqués. Une clé CMK ou un groupe de clés CMK est sélectionné pour vous, mais vous pouvez choisir les clés CMK si vous le souhaitez. Pour obtenir des informations sur l'utilisation de AWS KMS avec la réplication, veuillez consulter [Réplication d'objets créés à l'aide du chiffrement côté serveur \(SSE\) au moyen de clés de chiffrement stockées dans AWS KMS](#), dans le Amazon Simple Storage Service Manuel du développeur.



### Important

Lorsque vous répliquez des objets qui sont chiffrés avec AWS KMS, le taux de demandes AWS KMS double dans la région source et augmente dans la région de destination dans les mêmes proportions. Ces taux d'appel accrus vers AWS KMS sont dus à la manière dont les données sont chiffrées à nouveau à l'aide de la clé principale client (CMK) que vous définissez pour la région de destination de la répliquations. AWS KMS possède une limite de taux de demande par compte d'appel et par région. Pour plus d'informations sur les limites par défaut, consultez [Limites AWS KMS - Nombre de demandes par seconde : variable](#) dans le AWS Key Management Service Developer Guide.

Si votre taux de demandes d'objet PUT Amazon S3 actuel lors de la réplication est supérieur à la moitié de la limite de taux AWS KMS par défaut pour votre compte, nous vous recommandons de demander une augmentation de votre limite de taux de demandes AWS KMS. Pour demander une augmentation, [contactez-nous](#) pour créer une demande auprès de l'AWS Support Center. Par exemple, supposons que votre taux de demandes d'objet PUT actuel est de 1 000 demandes par seconde et que vous utilisez AWS KMS pour chiffrer vos objets. Dans ce cas, nous vous recommandons de demander à AWS Support d'augmenter votre limite de taux de demandes AWS KMS à 2 500 demandes par seconde pour vos régions source et de destination (s'il s'agit de régions différentes) afin de vous assurer qu'aucune limitation ne sera appliquée par AWS KMS.

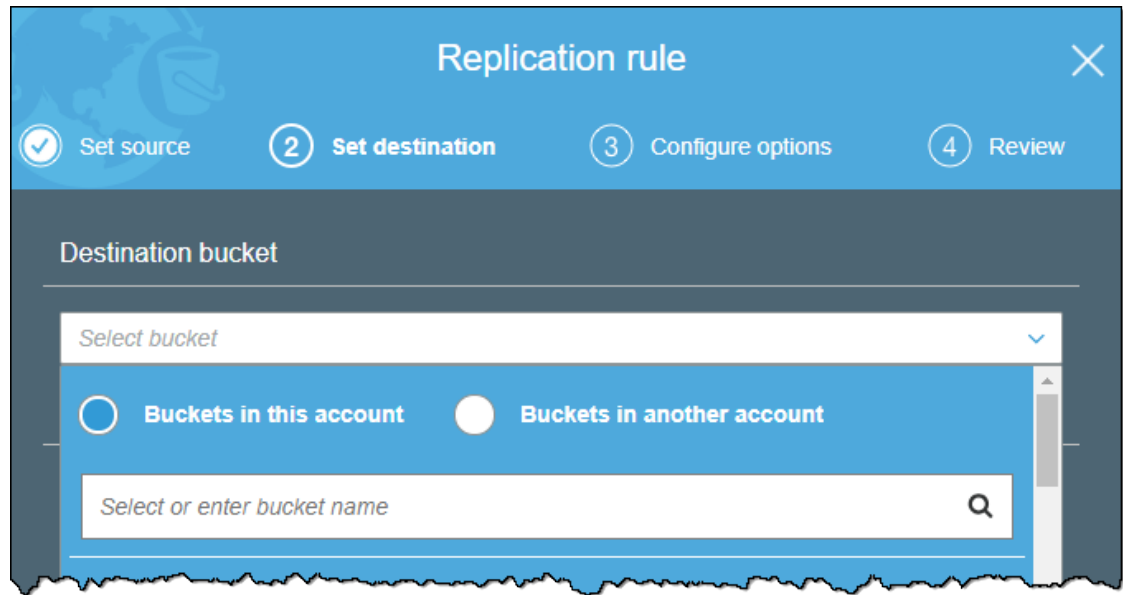
Pour consulter votre taux de demandes d'objet PUT dans le compartiment source, affichez `PutRequests` dans les métriques de demande Amazon CloudWatch pour Amazon S3. Pour plus d'informations sur l'affichage des métriques CloudWatch, consultez [Comment créer un filtre de métriques des demandes pour tous les objets de mon compartiment S3 ?](#) (p. 114)

Choisissez Suivant.

6. Pour choisir un compartiment de destination dans le compte que vous utilisez actuellement, sur la page Définir la destination, sous Compartiment de destination, choisissez Compartiments de ce compte. Saisissez le nom du compartiment de destination pour la réplication, ou choisissez un nom dans la liste déroulante.

Si vous souhaitez choisir un compartiment de destination à partir d'un autre compte AWS, consultez [Ajout d'une règle de réplication lorsque le compartiment de destination est dans un compte AWS distinct](#) (p. 96).





Si la gestion des versions n'est pas activée sur le compartiment de destination, un message d'avertissement contenant le bouton Activer la gestion des versions s'affiche. Cliquez sur ce bouton pour activer la gestion des versions sur le compartiment.

7. Si vous avez choisi de répliquer des objets chiffrés avec AWS KMS, sous Destination encryption settings (Paramètres de chiffrement de la destination), saisissez l'Amazon Resource Name (ARN) de la clé CMK AWS KMS à utiliser pour chiffrer les répliques dans le compartiment de destination. Vous trouverez l'ARN de votre clé CMK AWS KMS dans la console IAM sous Encryption keys (Clés de chiffrement). Ou, vous pouvez également choisir un nom de clé CMK dans la liste déroulante.

Pour plus d'informations sur la création d'une clé CMK AWS KMS, consultez [Création de clés](#) dans le AWS Key Management Service Developer Guide.

#### Important

La console Amazon S3 répertorie uniquement 100 clés CMK AWS KMS par région AWS. Si vous avez plus de 100 clés CMK dans la même région, vous ne pouvez voir que les 100 premières CMK dans la console S3. Pour utiliser une clé CMK KMS qui n'est pas répertoriée dans la console, choisissez ARN KMS personnalisé, puis saisissez l'ARN CMK KMS.

Destination encryption settings

AWS KMS key for destination objects

Type a KMS key ARN

Type to search

aws/s3

north-ca-key

Previous Next

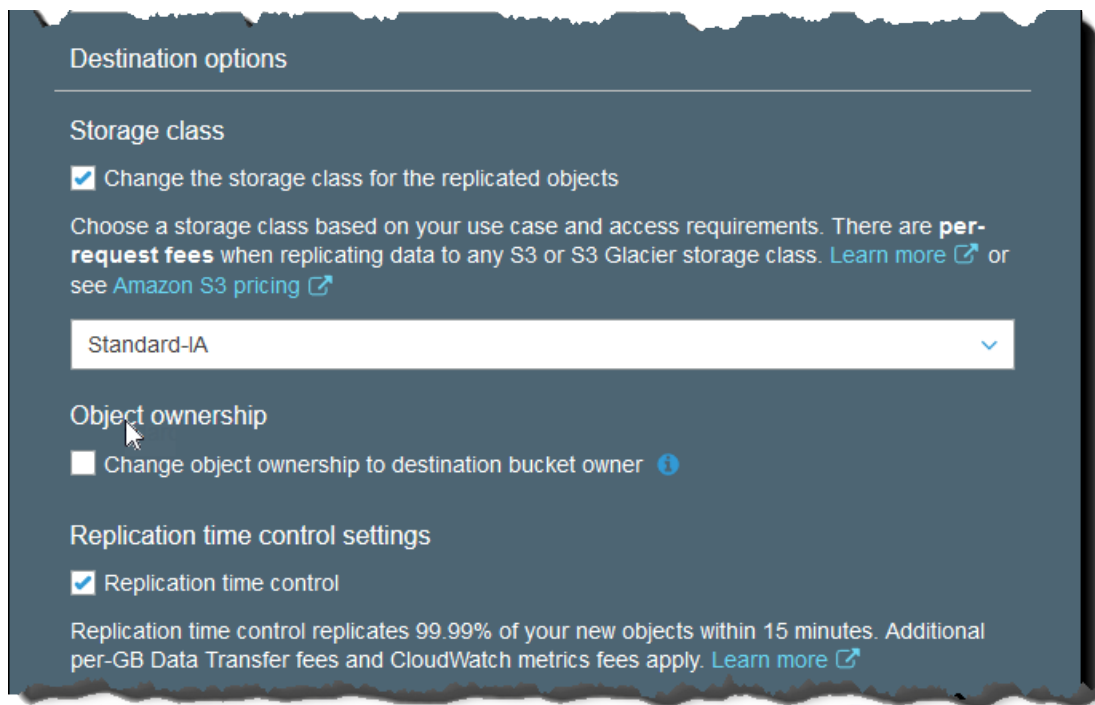
8. Si vous souhaitez répliquer vos données dans une classe de stockage spécifique dans le compartiment de destination, sur la page Définir la destination, sous Options de destination, sélectionnez Modifier la classe de stockage pour le ou les objets répliqués. Choisissez ensuite la classe de stockage que vous voulez utiliser pour les objets répliqués dans le compartiment de destination. Si vous ne sélectionnez pas cette option, la classe de stockage utilisée pour les objets répliqués est identique à celle des objets d'origine.

De même, si vous souhaitez modifier la propriété des objets dans le compartiment de destination, sélectionnez Change object ownership to the destination bucket owner (Modifier la propriété de l'objet en propriétaire du compartiment de destination). Pour plus d'informations sur cette option, consultez [Ajout d'une règle de réplication lorsque le compartiment de destination est dans un compte AWS distinct](#) (p. 96).

Si vous souhaitez activer S3 Replication Time Control (S3 RTC) dans votre configuration de réplication, sélectionnez Replication time control.

#### Note

Lorsque vous utilisez S3 RTC, des frais supplémentaires de transfert de données par Go et des frais de métriques CloudWatch s'appliquent.



Choisissez Suivant.

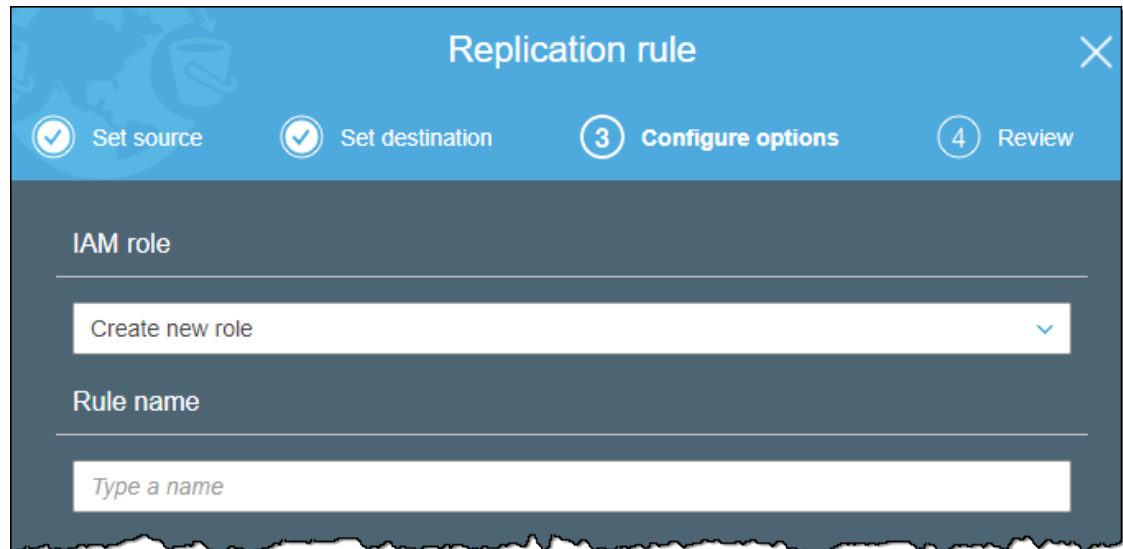
9. Définissez un rôle AWS Identity and Access Management (IAM) pouvant être endossé par Amazon S3 pour répliquer les objets en votre nom

Pour configurer un rôle IAM, sur la page Configurer les options, sous Sélectionner un rôle, exécutez l'une des actions suivantes :

- Nous vous recommandons vivement de choisir Créer un nouveau rôle pour demander à Amazon S3 de créer un rôle IAM pour vous. Lorsque vous enregistrez la règle, une nouvelle stratégie est générée pour le rôle IAM correspondant aux compartiments source et cible que vous choisissez. Le nom du rôle généré est basé sur les noms des compartiments et utilise la convention de dénomination suivante : rôle\_réplication\_pour\_**compartiment-source**\_vers\_**compartiment-destination**.
- Vous pouvez également choisir d'utiliser un rôle IAM existant. Dans ce cas, vous devez choisir un rôle qui octroie à Amazon S3 les autorisations nécessaires pour la réplication. La réplication échoue si ce rôle n'accorde pas à Amazon S3 des autorisations suffisantes pour suivre votre règle de réplication.

### Important

Lorsque vous ajoutez une règle de réplication à un compartiment, vous devez disposer de l'autorisation `iam:PassRole` pour pouvoir transmettre le rôle IAM qui accorde les autorisations de réplication Amazon S3. Pour plus d'informations, consultez [Octroi d'autorisations à un utilisateur pour transférer un rôle à un service AWS](#) dans le IAM Guide de l'utilisateur.

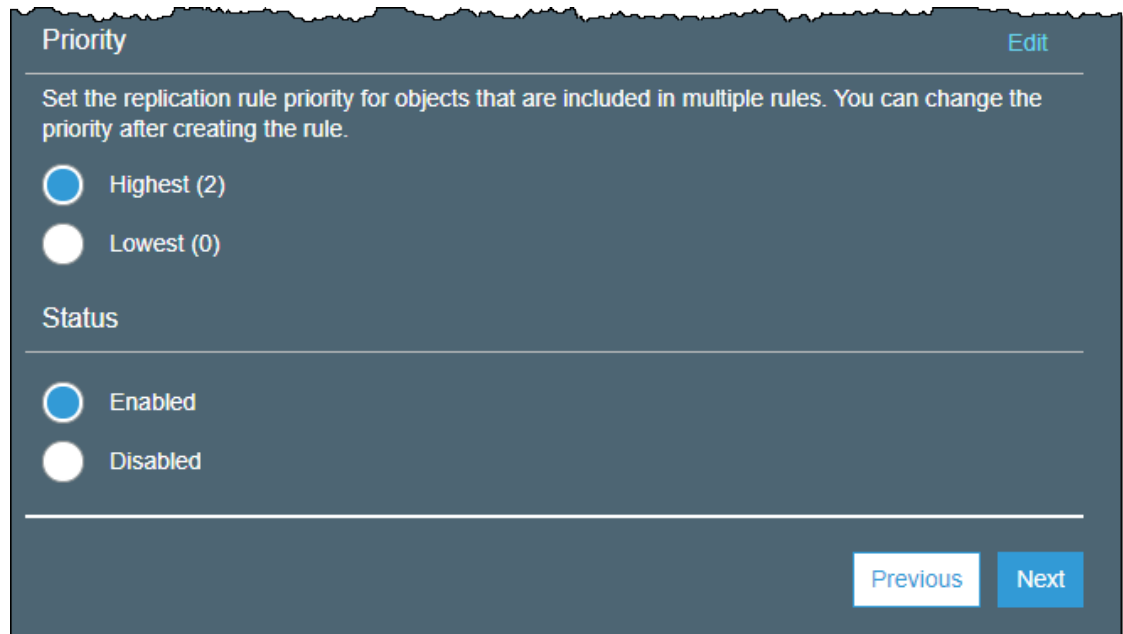


Sous Nom de la règle, attribuez un nom à votre règle afin de l'identifier facilement plus tard. Ce nom est obligatoire et doit être unique dans le compartiment.

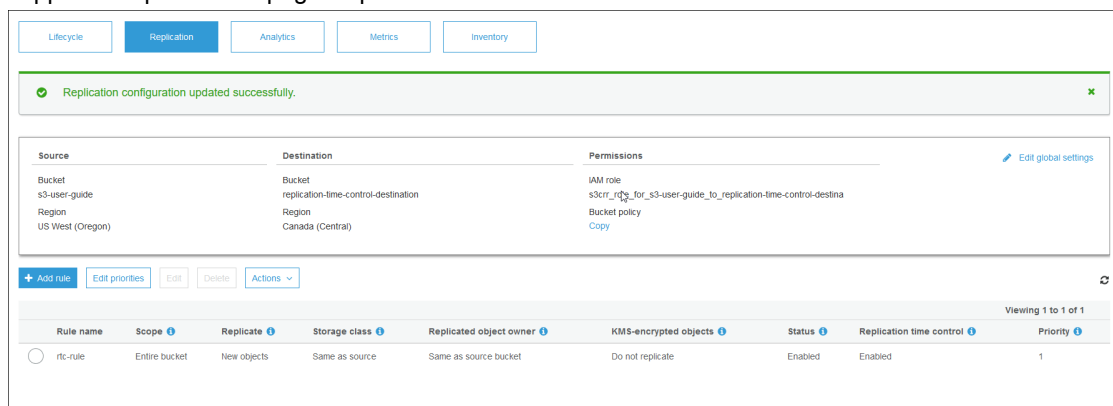
10. Si le compartiment possède des règles de réplication existantes, il vous est demandé de définir une priorité pour la règle. Vous devez définir une priorité pour la règle pour éviter les conflits provoqués par les objets inclus dans l'étendue de plusieurs règles. En cas de chevauchement de règles, Amazon S3 utilise la priorité des règles pour déterminer la règle à appliquer. Plus le nombre est élevé, plus la priorité est haute. Pour de plus amples informations sur la priorité des règles, veuillez consulter [Présentation de la configuration de la réplication](#) dans le Amazon Simple Storage Service Manuel du développeur.

Sous Statut, Activé est sélectionné par défaut. Une règle activée entre en fonctionnement dès que l'avez enregistrée. Si vous souhaitez activer la règle ultérieurement, sélectionnez Désactivé.

Choisissez Suivant.



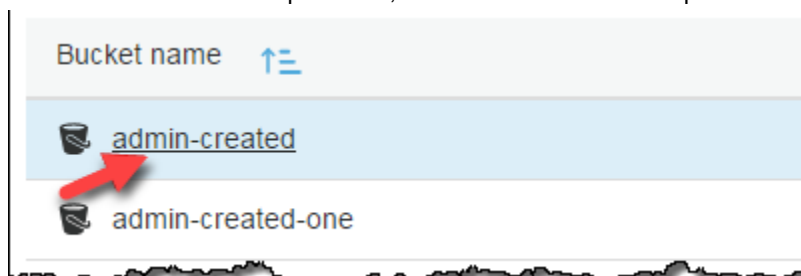
11. Sur la page Révision, vérifiez votre règle de réplication. Si elle vous semble correcte, choisissez Enregistrer. Sinon, choisissez Précédent pour modifier la règle avant de l'enregistrer.
12. Une fois que vous avez enregistré votre règle, vous pouvez la modifier, l'activer, la désactiver ou la supprimer à partir de la page Réplication.



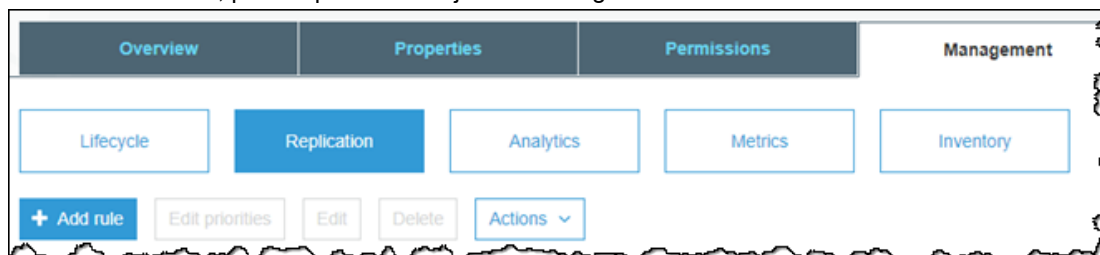
## Ajout d'une règle de réplication lorsque le compartiment de destination est dans un compte AWS distinct

Suivez ces étapes pour configurer une règle de réplication quand le compartiment de destination se trouve dans un compte AWS différent de celui du compartiment source.

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.



3. Choisissez Gestion, puis Réplication et Ajouter une règle.

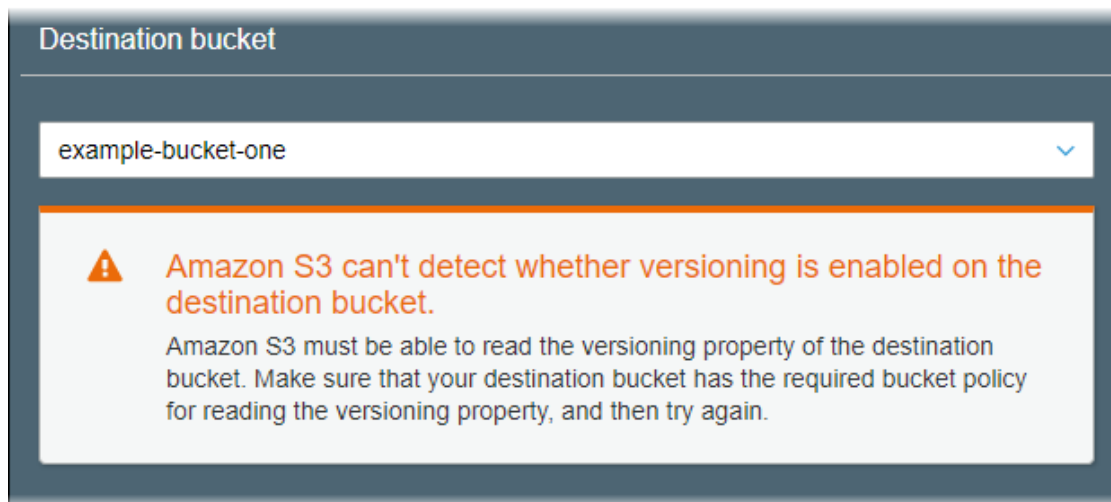


4. Si vous n'avez jamais créé de règle de réplication auparavant, commencez par [Ajout d'une règle de réplication lorsque le compartiment de destination est dans le même compte AWS](#) (p. 89).

Sur la page Définir une destination de l'assistant Règle de réplication, sous Compartiment de destination, choisissez Compartiments d'un autre compte. Entrez ensuite le nom du compartiment de destination et l'ID de compte d'un autre compte AWS. Choisissez Save.

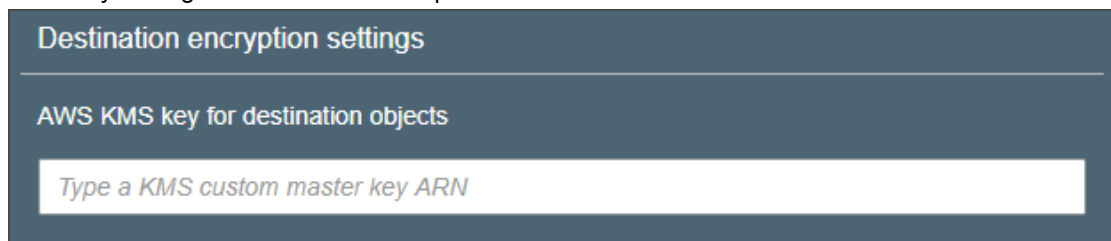
The screenshot shows the 'Replication rule' wizard in the AWS Management Console. The current step is '2 Set destination'. The 'Destination bucket' section is active. A dropdown menu is set to 'Select bucket'. Below it, the 'Buckets in another account' radio button is selected. The 'Account ID' field contains '111122223333' and the 'Bucket name' field contains 'example-bucket-one'. A 'Save' button is at the bottom of the form.

Après l'enregistrement du nom du compartiment de destination et de l'ID du compte, il est possible qu'un message d'avertissement s'affiche pour vous demander d'ajouter une stratégie de compartiment au compartiment de destination de sorte qu'Amazon S3 puisse vérifier si la gestion des versions est activée sur ce compartiment. Une stratégie de compartiment vous est présentée en quelques étapes que vous pouvez copier et ajouter au compartiment de destination dans l'autre compte. Pour plus d'informations sur l'ajout d'une stratégie de compartiment à un compartiment S3 et la gestion des versions, consultez [Comment ajouter une stratégie de compartiment S3 ? \(p. 131\)](#) et [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#)



5. Si vous avez choisi de répliquer les objets chiffrés avec AWS KMS, sous Paramètres de chiffrement de la destination, saisissez l'Amazon Resource Name (ARN) de la clé CMK AWS KMS à utiliser pour chiffrer les répliques dans le compartiment de destination.

Pour plus d'informations sur la création d'une clé CMK AWS KMS, consultez [Création de clés](#) dans le AWS Key Management Service Developer Guide.



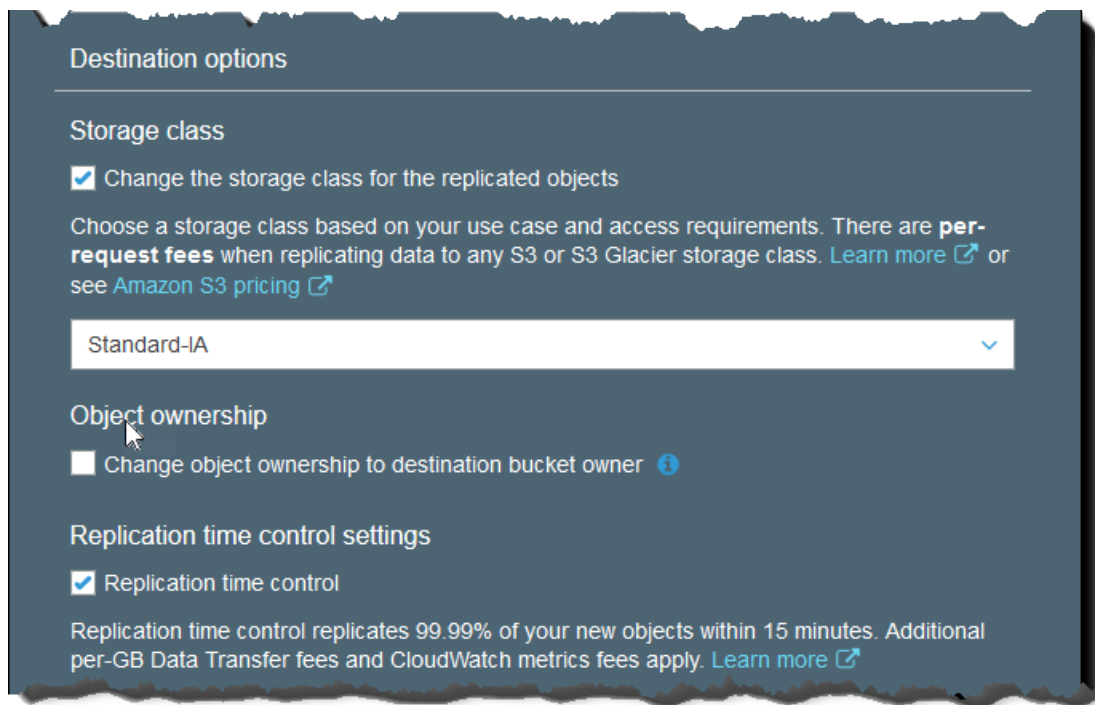
6. Sur la page Définir la destination sous Options de destination :
  - Pour répliquer vos données dans une classe de stockage spécifique dans le compartiment de destination, sélectionnez Modifier la classe de stockage pour le ou les objets répliqués. Choisissez ensuite la classe de stockage que vous voulez utiliser pour les objets répliqués dans le compartiment de destination. Si vous ne sélectionnez pas cette option, la classe de stockage utilisée pour les objets répliqués est identique à celle des objets d'origine.
  - Pour modifier la propriété des objets de réplica en propriétaire du compartiment de destination, sélectionnez Modifier la propriété de l'objet en faveur du propriétaire du compartiment de destination. Cette option vous permet de séparer la propriété d'objet des données répliquées de la source. Si vous y êtes invité, saisissez l'ID du compartiment de destination.

Quand vous sélectionnez cette option, quel que soit le propriétaire du compartiment ou de l'objet source, le compte AWS qui possède le compartiment de destination se voit accorder l'intégralité des autorisations sur les objets réplica. Pour plus d'informations, consultez [Modification du propriétaire d'un réplica](#) dans le Amazon Simple Storage Service Manuel du développeur.

- Si vous souhaitez ajouter S3 Replication Time Control (S3 RTC) à votre configuration de réplication, sélectionnez Replication time control.

#### Note

Lorsque vous utilisez S3 RTC, des frais supplémentaires de transfert de données par Go et des frais de métriques CloudWatch s'appliquent.



Choisissez Suivant.

7. Configurez un rôle AWS Identity and Access Management (IAM) qu'Amazon S3 peut assumer pour effectuer des réplications d'objets en votre nom.

Pour configurer un rôle IAM, sur la page Configurer les options, sous Sélectionner un rôle, exécutez l'une des actions suivantes :

- Nous vous recommandons vivement de choisir Créer un nouveau rôle pour demander à Amazon S3 de créer un rôle IAM pour vous. Lorsque vous enregistrez la règle, une nouvelle stratégie est générée pour le rôle IAM correspondant aux compartiments source et cible que vous choisissez. Le nom du rôle généré est basé sur les noms des compartiments et utilise la convention de dénomination suivante : rôle\_réplication\_pour\_**compartiment-source**\_vers\_**compartiment-destination**.
- Vous pouvez également choisir d'utiliser un rôle IAM existant. Dans ce cas, vous devez choisir un rôle qui permet à Amazon S3 de répliquer des objets à partir du compartiment source vers le compartiment de destination en votre nom.



Replication rule

Set source Set destination **3 Configure options** 4 Review

IAM role

Create new role

Rule name

Type a name

Status

Enabled Disabled

8. Une stratégie de compartiment est fournie sur la page Configurer les options que vous pouvez copier et ajouter au compartiment de destination de l'autre compte. Pour plus d'informations sur l'ajout d'une stratégie de compartiment à un compartiment S3, consultez [Comment ajouter une stratégie de compartiment S3 ?](#) (p. 131)

Bucket policy

Amazon S3 requires you to put the following policy in the destination bucket.

Bucket policy Copy

```
1 {
2   "Version": "2008-10-17",
3   "Id": "S3-Console-Replication-Policy",
4   "Statement": [
5     {
6       "Sid": "S3ReplicationPolicyStmt1",
7       "Effect": "Allow",
8       "Principal": {
9         "AWS": "arn:aws:iam::444455556666 :root"
10      },
11      "Action": [
12        "s3:GetBucketVersioning",
13        "s3:PutBucketVersioning",
14        "s3:ReplicateObject",
15        "s3:ReplicateDelete"
16      ],
17      "Resource": [
```

Previous Next

- Si vous avez choisi de répliquer les objets chiffrés avec AWS KMS, une stratégie de clé AWS KMS est fournie sur la page Configurer les options. Vous pouvez copier cette stratégie pour l'ajouter à la stratégie de clé de la clé CMK AWS KMS que vous utilisez. La stratégie de clé accorde au propriétaire du compartiment source l'autorisation d'utiliser la clé. Pour plus d'informations sur la mise à jour de la stratégie de clé, consultez [Octroi au propriétaire du compartiment source de l'autorisation de chiffrer à l'aide de la clé CMK AWS KMS](#) (p. 103).

### KMS key policy

Before saving KMS encryption settings, ensure that all producers and consumers have access to the specified encryption key. You can choose Copy to copy and paste policy to the KMS key. [Learn more](#)

KMS key policy [Copy](#)

```
1 {
2   "Sid": "Enable cross account encrypt access for S3 Cross Region Replication",
3   "Effect": "Allow",
4   "Principal": {
5     "AWS": "*"
6   },
7   "Action": [
8     "kms:Encrypt"
9   ],
10  "Resource": "*"
11 }
```

[Previous](#) [Next](#)

- Sur la page Révision, vérifiez votre règle de réplication. Si elle vous semble correcte, choisissez Enregistrer. Sinon, choisissez Précédent pour modifier la règle avant de l'enregistrer.
- Une fois que vous avez enregistré votre règle, vous pouvez la modifier, l'activer, la désactiver ou la supprimer à partir de la page Réplication.

[Lifecycle](#) [Replication](#) [Analytics](#) [Metrics](#) [Inventory](#)

✓ Replication configuration updated successfully.

Source	Destination	Permissions
Bucket s3-user-guide	Bucket replication-time-control-destination	IAM role s3crr_rdg_for_s3-user-guide_to_replication-time-control-destina
Region US West (Oregon)	Region Canada (Central)	Bucket policy <a href="#">Copy</a>

[+ Add rule](#) [Edit priorities](#) [Edit](#) [Delete](#) [Actions](#)

Rule name	Scope	Replicate	Storage class	Replicated object owner	KMS-encrypted objects	Status	Replication time control	Priority
rtc-rule	Entire bucket	New objects	Same as source	Destination bucket owner	Do not replicate	Enabled	Enabled	1

Viewing 1 to 1 of 1

- Suivez les instructions figurant sur la page Réplication sous le message d'avertissement The replication rule is saved, but additional settings are required in the destination account (La règle de réplication est enregistrée, mais des paramètres supplémentaires sont nécessaires dans le compte de destination). Déconnectez-vous du compte AWS auquel vous êtes actuellement connecté, puis vous reconnectez-vous au compte de destination.

## Important

La réplication échoue tant que vous ne vous êtes pas connecté au compte de destination et que vous n'avez pas exécuté les étapes suivantes.

13. Après vous être connecté au compte de destination, choisissez l'onglet Gestion, sélectionnez Réplication, puis choisissez Recevoir les objets dans le menu Actions.
14. Sur la page Recevoir des objets, vous pouvez effectuer les opérations suivantes :
  - Activer la gestion des versions sur le compartiment de destination.
  - Appliquer la stratégie de compartiment fournie par Amazon S3 au compartiment de destination.
  - Copiez la stratégie de clé AWS KMS dont vous avez besoin pour mettre à jour la clé CMK AWS KMS utilisée pour chiffrer les objets répliqués dans le compartiment de destination. Pour plus d'informations sur la mise à jour de la stratégie de clé, consultez [Octroi au propriétaire du compartiment source de l'autorisation de chiffrer à l'aide de la clé CMK AWS KMS](#) (p. 103).

### Receive objects

To use this bucket as the destination for replicated objects, type the your source account ID. Then configure the policy settings that are required to receive objects in this bucket.

#### Versioning

If you don't have versioning enabled for this bucket, S3 enables it for you.

► Bucket policy

Copy

Apply settings

▼ KMS policy

Copy

```
1 {
2   "Sid": "Enable cross account encrypt access for S3 Cross Region Replication",
3   "Effect": "Allow",
4   "Principal": {
5     "AWS": "SOURCE_ACCOUNT_ID"
6   },
7   "Action": [
8     "kms:Encrypt"
9   ],
10  "Resource": "*"
11 }
```

Done

## Octroi au propriétaire du compartiment source de l'autorisation de chiffrer à l'aide de la clé CMK AWS KMS

Vous devez autoriser le compte du propriétaire du compartiment source à chiffrer à l'aide de votre clé AWS KMS avec une stratégie de clé. La procédure suivante montre comment utiliser la console AWS Identity and Access Management (IAM) afin de modifier la stratégie de clé pour la clé CMK AWS KMS qui est utilisée pour chiffrer les objets réplica dans le compartiment de destination.

Pour accorder l'autorisation de chiffrer à l'aide de votre clé CMK AWS KMS

1. Connectez-vous à la AWS Management Console à l'aide du compte AWS qui possède la clé CMK AWS KMS. Ouvrez la console AWS KMS à l'adresse <https://console.aws.amazon.com/kms>.
2. Choisissez l'alias de la clé CMK avec laquelle vous souhaitez chiffrer.
3. Dans la section Stratégie de clé de la page, choisissez Passer à la vue de stratégie.
4. Choisissez Modifier pour modifier la stratégie de clé.
5. À l'aide de l'éditeur Stratégie de clé, insérez la stratégie de clé fournie par Amazon S3 dans la stratégie de clé existante, puis choisissez Enregistrer les modifications. Vous pouvez ajouter la stratégie à la fin de la stratégie existante.

Pour plus d'informations sur la création et la modification des clés CMK AWS KMS, consultez [Mise en route](#) dans le AWS Key Management Service Developer Guide.

## Plus d'informations

- [Comment gérer les règles de réplication pour un compartiment S3 ? \(p. 103\)](#)
- [Comment activer ou interrompre la gestion des versions d'un compartiment S3 ? \(p. 8\)](#)
- [Réplication](#) dans le Amazon Simple Storage Service Manuel du développeur

## Comment gérer les règles de réplication pour un compartiment S3 ?

La réplication est une fonctionnalité qui permet la copie d'objets automatique et asynchrone entre les compartiments de différentes régions AWS ou d'une même région AWS. Elle réplique les objets nouvellement créés et les mises à jour d'objets d'un compartiment source vers un compartiment de destination spécifié.

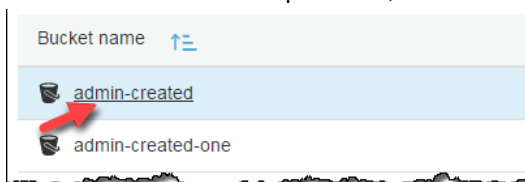
Utilisez la console Amazon S3 pour ajouter des règles de réplication dans le compartiment source. Les règles de réplication définissent les objets du compartiment source à répliquer, ainsi que le compartiment de destination dans lequel les objets répliqués seront stockés. Pour de plus amples informations sur la réplication, veuillez consulter [Réplication](#) dans le Amazon Simple Storage Service Manuel du développeur.

Vous pouvez gérer les règles de réplication sur la page Réplication. Vous pouvez ajouter, afficher, activer, désactiver et changer la priorité des règles de réplication. Pour plus d'informations sur l'ajout de règles de réplication à un compartiment, consultez [Comment ajouter une règle de réplication à un compartiment S3 ? \(p. 87\)](#).

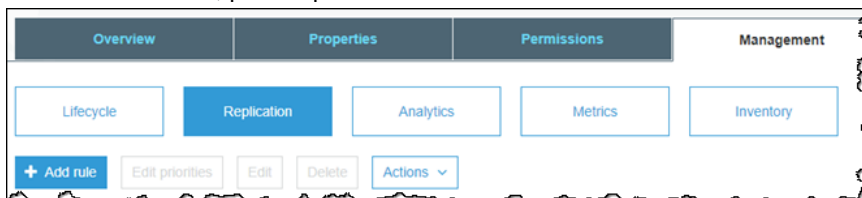
Pour gérer les règles de réplication pour un compartiment S3

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

2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.



3. Choisissez Gestion, puis Réplication.



4. Vous pouvez modifier les règles de réplication de différentes manières :

- Pour modifier les paramètres qui affectent toutes les règles de réplication du compartiment, choisissez Modifier les paramètres globaux.

Source	Destination	Permissions	<a href="#">Edit global settings</a>
Bucket admin-created	Bucket ca-example-bucket	IAM role s3crr_role_for_admin-created_to_ca-example-bucket	
Region US West (Oregon)	Region US West (N. California)	Bucket policy <a href="#">Copy</a>	

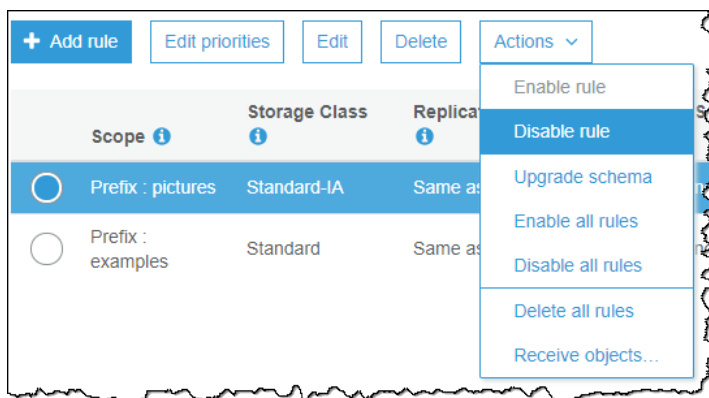
Vous pouvez modifier le compartiment de destination et le rôle IAM. Si nécessaire, vous pouvez copier la stratégie de compartiment requise pour les compartiments de destination entre comptes.

Source	Destination	Permissions	<a href="#">Cancel</a>	<a href="#">Save</a>
Bucket admin-created	Bucket <div>ca-example-bucket</div>	IAM role <div>s3crr_role_for_admin-...</div>		
Region US West (Oregon)		Bucket policy <a href="#">Copy</a>		

- Pour modifier une règle de réplication, sélectionnez-la et choisissez Modifier ; l'assistant de réplication démarre pour vous aider à effectuer la modification. Pour plus d'informations sur l'utilisation de l'assistant, consultez la section [Comment ajouter une règle de réplication à un compartiment S3 ?](#) (p. 87).

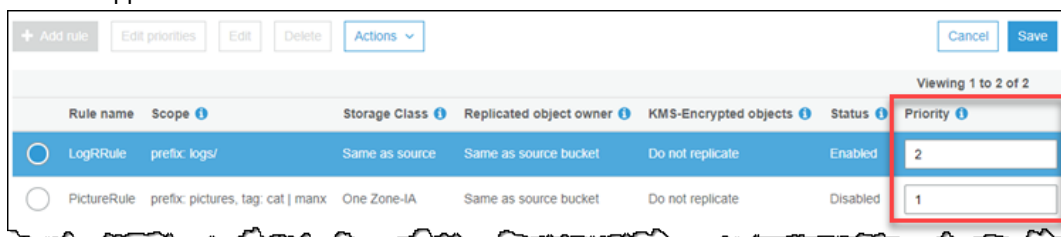
<a href="#">+ Add rule</a>	<a href="#">Edit priorities</a>	<a href="#">Edit</a>	<a href="#">Delete</a>	<a href="#">Actions</a>
Scope	Storage Class	Replicated object owner		
<input checked="" type="radio"/> Prefix : pictures	Standard-IA	Same as source bucket		
<input type="radio"/> Prefix : examples	Standard	Same as source bucket		

- Pour activer ou désactiver une règle de réplication, sélectionnez-la, choisissez Plus puis, dans la liste déroulante, choisissez Activer une règle ou Désactiver une règle. Vous pouvez également désactiver, activer ou supprimer toutes les règles du compartiment à partir de la liste déroulante Plus.



- Pour modifier les priorités des règles, choisissez Edit priorities (Modifier les priorités). Vous pouvez alors modifier la priorité de chaque règle sous l'en-tête de colonne Priorité. Choisissez Save pour enregistrer les changements.

Vous devez définir les priorités des règles pour éviter les conflits provoqués par les objets inclus dans l'étendue de plusieurs règles. En cas de chevauchement de règles, Amazon S3 utilise la priorité des règles pour déterminer la règle à appliquer. Plus le nombre est élevé, plus la priorité est haute. Pour de plus amples informations sur la priorité des règles, veuillez consulter [Présentation de la configuration de la réplication](#) dans le Amazon Simple Storage Service Manuel du développeur.



## Plus d'informations

- [Comment ajouter une règle de réplication à un compartiment S3 ? \(p. 87\)](#)
- [Réplication](#) dans le Amazon Simple Storage Service Manuel du développeur

## Comment configurer une analyse de classe de stockage ?

Grâce à l'outil d'analyse de classe de stockage Amazon S3, vous pouvez analyser des modèles d'accès au stockage pour décider à quel moment transférer les données appropriées vers la classe de stockage qui convient. L'analyse de classe de stockage observe les modèles d'accès aux données pour vous aider à déterminer quand il faut passer du mode STANDARD au mode STANDARD\_IA (« IA » correspondant à « infrequent access », soit accès peu fréquent). Pour de plus amples informations sur STANDARD\_IA, veuillez consulter la [Amazon S3 FAQ](#) et la rubrique [Classes de stockage](#) du Amazon Simple Storage Service Manuel du développeur.

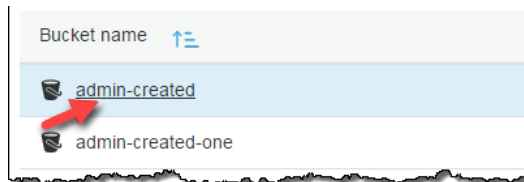
### Important

L'analyse de classe de stockage ne fournit pas de recommandations pour les transitions vers les classes de stockage ONEZONE\_IA ou S3 Glacier.

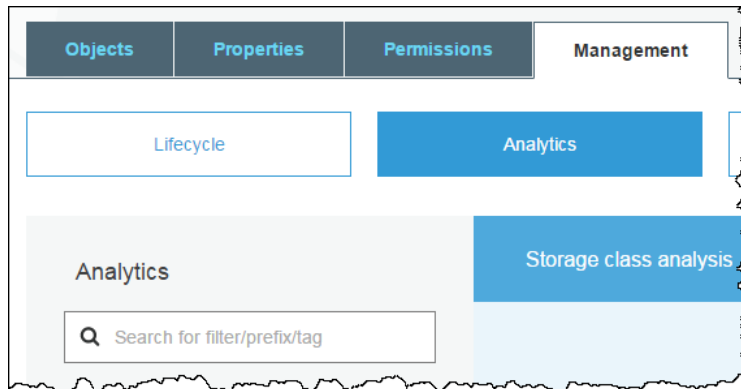
Pour de plus amples informations sur l'analyse, consultez [Analyses Amazon S3 – Analyse de classe de stockage](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour configurer une analyse de classe de stockage

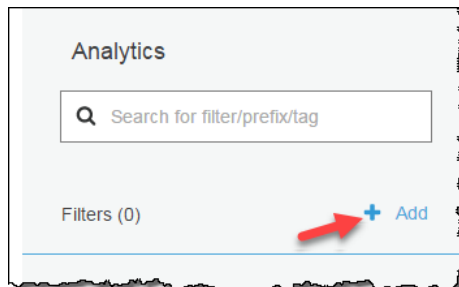
1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez configurer une analyse de classe de stockage.



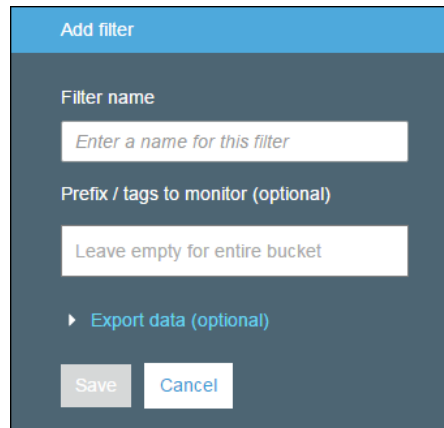
3. Choisissez l'onglet Management, puis choisissez Analytics.



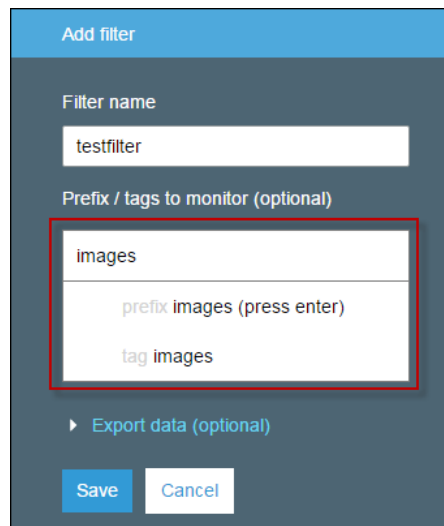
4. Choisissez Ajouter.



5. Attribuez un nom au filtre. Pour analyser le compartiment entier, n'indiquez rien dans le champ Prefix / tags .

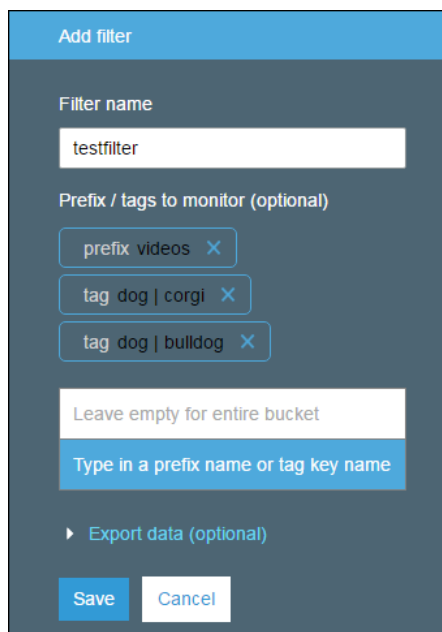


6. Dans le champ Prefix / tags , saisissez le texte du préfixe ou de la balise des objets à analyser, ou choisissez une entrée dans la liste déroulante qui s'affiche lorsque vous commencez à saisir cette information.

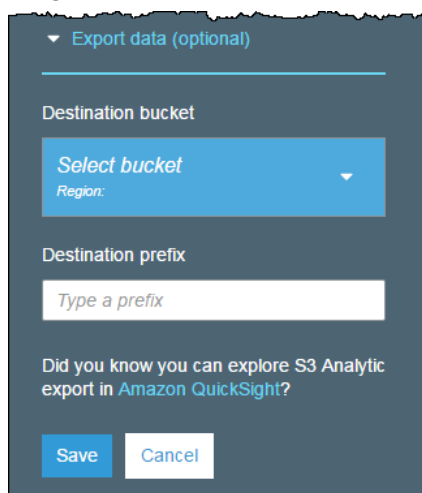


7. Si vous choisissez tag, saisissez une valeur pour la balise. Vous pouvez entrer un préfixe et plusieurs balises.





8. Vous pouvez également choisir Export data pour exporter des rapports d'analyse au format de fichier plat CSV (valeurs séparées par une virgule). Choisissez un compartiment de destination dans lequel le fichier peut être stocké. Vous pouvez saisir un préfixe pour le compartiment de destination. Le compartiment de destination doit se trouver dans la même région AWS que le compartiment pour lequel vous configurez l'analyse. Le compartiment de destination peut se trouver dans un autre compte AWS.



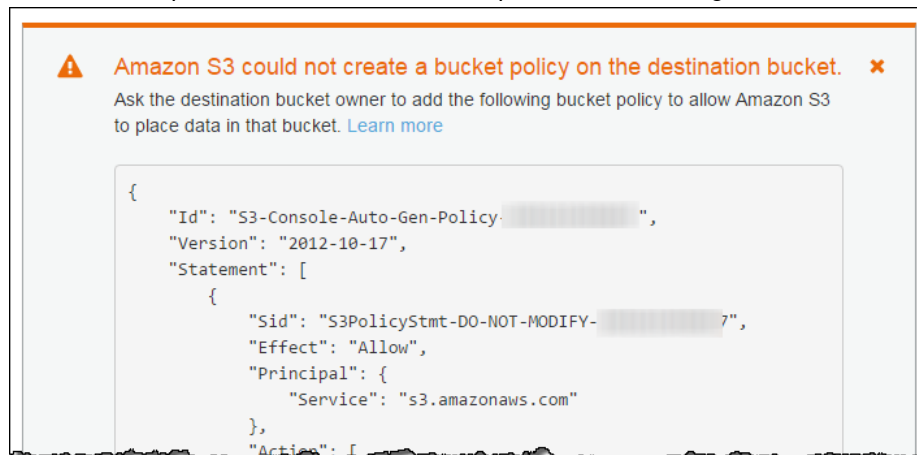
9. Choisissez Save.

Amazon S3 crée une stratégie de compartiment sur le compartiment de destination qui accorde à Amazon S3 une autorisation en écriture. Cela l'autorise à écrire les données d'exportation dans le compartiment.

#### Note

Cette action configure l'analyse de la classe de stockage pour tous les compartiments spécifiés.

Si une erreur se produit lorsque vous tentez de créer la stratégie de compartiment, des instructions s'affichent pour vous indiquer comment la résoudre. Par exemple, si vous avez choisi un compartiment de destination dans un autre compte AWS et ne disposez pas des autorisations nécessaires pour lire et écrire dans la stratégie de compartiment, le message suivant s'affiche. Vous devez demander au propriétaire du compartiment de destination d'ajouter la stratégie de compartiment affichée au compartiment de destination. Si la stratégie n'est pas ajoutée au compartiment de destination, vous ne recevez pas les données d'exportation, car Amazon S3 n'est pas autorisé à écrire dans le compartiment de destination. Si le compartiment source est détenu par un compte autre que celui de l'utilisateur actuel, l'ID de compte correct du compartiment source doit être remplacé dans la stratégie.



Pour en savoir plus sur les données exportées et le fonctionnement du filtre, consultez [Analyses Amazon S3 – Analyse de classe de stockage](#) dans le Amazon Simple Storage Service Manuel du développeur.

Plus d'informations

[Gestion du stockage \(p. 83\)](#)

## Comment configurer l'inventaire Amazon S3 ?

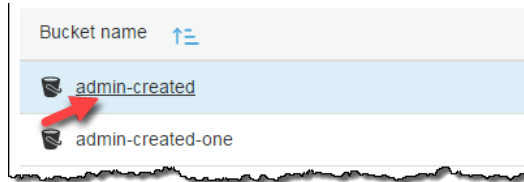
L'inventaire Amazon S3 fournit une liste de fichiers plats de vos objets et métadonnées, ce qui constitue une alternative planifiée à l'opération d'API Amazon S3 `List` synchrone. L'inventaire Amazon S3 fournit des fichiers de sortie au format CSV (valeurs séparées par une virgule), au [format ORC \(Optimized Row Columnar\) Apache](#) ou au [format Apache Parquet \(Parquet\)](#) qui répertorient vos objets et leurs métadonnées tous les jours ou toutes les semaines pour un compartiment S3 ou pour des objets partageant un même préfixe (objets dont le nom commence par la même chaîne). Pour plus d'informations, consultez [Inventaire Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour configurer un inventaire

### Note

La distribution du premier rapport peut prendre jusqu'à 48 heures.

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez configurer un inventaire Amazon S3.



3. Cliquez sur l'onglet Gestion, puis choisissez Inventaire.
4. Choisissez Add new (Ajouter nouveau).
5. Saisissez un nom d'inventaire et configurez ce dernier comme suit :
  - Vous pouvez également ajouter un préfixe à votre filtre afin d'inventorier uniquement les objets dont les noms commencent par la même chaîne.
  - Choisissez le compartiment de destination dans lequel vous souhaitez que les rapports soient enregistrés. Le compartiment de destination doit se trouver dans la même région AWS que le compartiment pour lequel vous configurez l'inventaire. Le compartiment de destination peut se trouver dans un autre compte AWS.
  - Vous pouvez également choisir un préfixe pour le compartiment de destination.
  - Choisissez la fréquence à laquelle l'inventaire sera généré.

A screenshot of the 'Add new' inventory configuration form in the Amazon S3 console. At the top are buttons for '+ Add new', 'Edit', and 'Delete'. Below is a table with five columns: 'Inventory name', 'Filters', 'Destination bucket', 'Destination prefix', and 'Frequency'. Under 'Inventory name' is a text input field with the placeholder 'Enter inventory name'. Under 'Filters' is a text input field with the placeholder 'Filter by prefix (optional)'. Under 'Destination bucket' is a blue button labeled 'Select bucket' with a dropdown arrow. Under 'Destination prefix' is a text input field with the placeholder 'Type prefix (optional)'. Under 'Frequency' is a dropdown menu currently set to 'Daily'.

6. Sous Paramètres avancés, vous pouvez définir les éléments suivants :
  - a. Choisissez le format de fichier de sortie CSV, ORC ou Parquet pour votre inventaire. Pour plus d'informations sur ces formats, consultez [Inventaire Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

- Advanced settings

**Output format** Choose an output format based on the number of objects that you expect to list or the analysis tool that you want to use. [Learn more](#)

☒ CSV  
Choose this format for listing 1 million or fewer objects, or if you plan to analyze S3 Inventory with tools like Excel.

☐ Apache ORC

☐ Apache Parquet

**Object versions** Current version only

**Optional fields**

- ☒ Size
- ☐ Last modified date
- ☒ Storage class
- ☐ Etag
- ☐ Multipart upload
- ☐ Replication status
- ☒ Encryption status
- ☒ All object lock configurations (3 selected)
  - ☒ Retention mode
  - ☒ Retain until date
  - ☒ Legal hold status

**Encryption**

☒ None

☐ AES-256

☐ AWS-KMS

[Cancel](#) [Save](#)

- b. Pour inclure toutes les versions des objets dans l'inventaire, choisissez Inclure toutes les versions dans la liste Versions d'objet. Par défaut, l'inventaire comprend uniquement la version actuelle des objets.
- c. Pour Champs facultatifs, sélectionnez un ou plusieurs des éléments suivants à ajouter au rapport d'inventaire :
- Taille – La taille des objets en octets.
  - Date de la dernière modification – Date de création de l'objet ou date de la dernière modification, la plus récente étant retenue.
  - Classe de stockage – Classe de stockage utilisé pour stocker l'objet.
  - ETag – La balise d'entité est un hachage de l'objet. ETag reflète les modifications apportées uniquement au contenu d'un objet, et non pas à ses métadonnées. ETag peut être ou ne pas être une valeur de hachage MD5 des données de l'objet. Cela dépend de la façon dont l'objet a été créé et de la manière dont il est chiffré.
  - Chargement partitionné – Spécifie que l'objet a été chargé dans un chargement partitionné. Pour plus d'informations, consultez [Présentation du chargement partitionné](#) dans le Amazon Simple Storage Service Manuel du développeur.
  - Statut de réplication – Statut de réplication de l'objet. Pour de plus amples informations, veuillez consulter [Comment ajouter une règle de réplication à un compartiment S3 ? \(p. 87\)](#).
  - Encryption status (Statut de chiffrement) – Le chiffrement côté serveur utilisé pour chiffrer l'objet. Pour plus d'informations, consultez [Protection des données à l'aide du chiffrement côté serveur](#) dans le Amazon Simple Storage Service Manuel du développeur.
  - ConfigurationsS3 Verrouillage d'objet – L'état Verrouillage d'objet de l'objet, y compris les paramètres suivants :
    - Retention mode (Mode de rétention) – Niveau de protection appliqué à l'objet, Gouvernance ou Conformité.
    - Retain until date (Date de fin de conservation) – Date avant laquelle l'objet verrouillé ne peut pas être supprimé.

- Legal hold status (Statut de détention légale) – Statut de détention légale de l'objet verrouillé.

Pour de plus amples informations sur S3 Verrouillage d'objet, veuillez consulter [Vue d'ensemble de S3 Verrouillage d'objet](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour plus d'informations sur le contenu d'un rapport d'inventaire, consultez [Qu'est-ce qui est inclus dans un inventaire Amazon S3 ?](#) dans le Amazon Simple Storage Service Manuel du développeur.

- d. Pour Chiffrement, choisissez une option de chiffrement côté serveur pour chiffrer le rapport d'inventaire, ou choisissez Aucun :
- Aucun – Ne pas chiffrer le rapport d'inventaire.
  - AES-256 – Chiffrer le rapport d'inventaire à l'aide du chiffrement côté serveur avec les clés gérées par Amazon S3 (SSE-S3). Le chiffrement côté serveur Amazon S3 utilise la norme Advanced Encryption Standard à 256 bits (AES-256). Pour plus d'informations, consultez [Clés de chiffrement gérées par Amazon S3 \(SSE-S3\)](#) dans le Amazon Simple Storage Service Manuel du développeur.
  - AWS-KMS – Chiffrer le rapport à l'aide du chiffrement côté serveur avec les clés CMK AWS Key Management Service (AWS KMS). Pour plus d'informations, consultez [Clés CMK AWS KMS](#) dans le Amazon Simple Storage Service Manuel du développeur.

#### Note

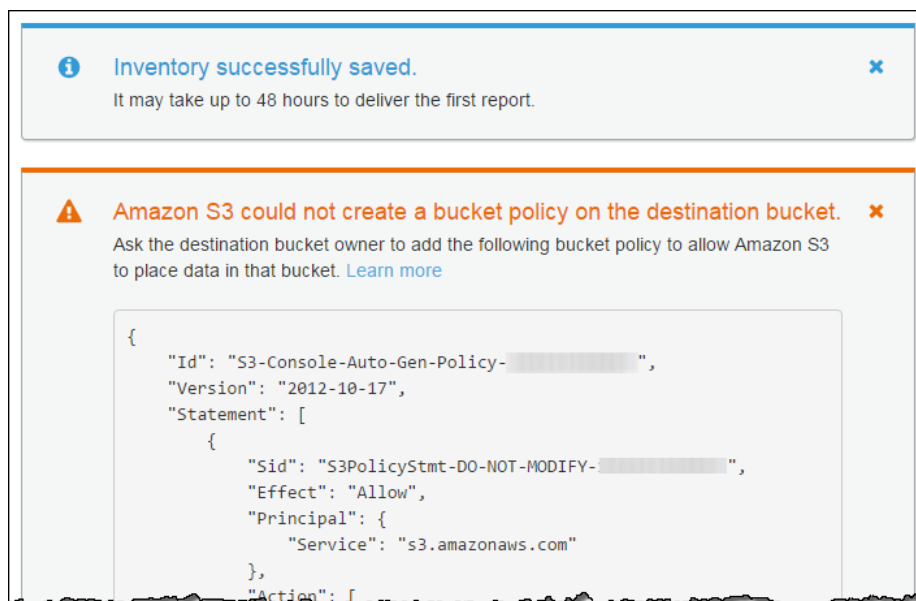
Pour chiffrer le fichier de listes d'inventaires avec SSE-KMS, vous devez autoriser Amazon S3 à utiliser la clé CMK AWS KMS. Pour plus d'instructions, consultez [Accorder à Amazon S3 l'autorisation de chiffrer avec votre clé CMK AWS KMS](#) (p. 113).

7. Choisissez Save.

## Stratégie du compartiment de destination

Amazon S3 crée une stratégie de compartiment sur le compartiment de destination qui accorde à Amazon S3 une autorisation en écriture. Cela autorise Amazon S3 à écrire des données pour les rapports d'inventaire dans le compartiment.

Si une erreur se produit lorsque vous tentez de créer la stratégie de compartiment, des instructions s'affichent pour vous indiquer comment la résoudre. Par exemple, si vous choisissez un compartiment de destination dans un autre compte AWS et ne disposez pas des autorisations nécessaires pour lire et écrire dans la stratégie de compartiment, le message suivant s'affiche.



Dans ce cas, le propriétaire du compartiment de destination doit ajouter la stratégie de compartiment affichée au compartiment de destination. Si la stratégie n'est pas ajoutée au compartiment de destination, vous ne recevez pas de rapport d'inventaire, car Amazon S3 n'est pas autorisé à écrire dans le compartiment de destination. Si le compartiment source est détenu par un compte autre que celui de l'utilisateur actuel, l'ID de compte correct du compartiment source doit être remplacé dans la stratégie.

Pour plus d'informations, consultez [Inventaire Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Autoriser Amazon S3 à utiliser votre CMK AWS KMS pour le chiffrement

Pour accorder à Amazon S3 l'autorisation de chiffrer à l'aide d'une clé principale client AWS Key Management Service (AWS KMS) gérée par le client (CMK), vous devez utiliser une stratégie de clé. Pour mettre à jour votre stratégie de clé et pouvoir utiliser une CMK AWS KMS gérée par le client pour chiffrer le fichier d'inventaire, procédez comme suit.

Pour accorder l'autorisation de chiffrer à l'aide de votre clé CMK AWS KMS

1. En utilisant le compte AWS propriétaire de la CMK gérée par le client, connectez-vous à la AWS Management Console.
2. Ouvrez la console AWS KMS à l'adresse <https://console.aws.amazon.com/kms>.
3. Pour changer de région AWS, utilisez le sélecteur de région dans l'angle supérieur droit de la page.
4. Dans le volet de navigation de gauche, choisissez Customer managed keys (Clés gérées par le client).
5. Sous Customer managed keys (Clés gérées par le client), choisissez la CMK gérée par le client que vous souhaitez utiliser pour chiffrer le fichier d'inventaire.
6. Sous Key policy (Stratégie de clé), choisissez Switch to policy view (Passer à la vue de stratégie).
7. Pour mettre à jour la stratégie de clé, choisissez Edit (Modifier).
8. Sous Edit key policy (Modifier la stratégie de clé), ajoutez la stratégie de clé suivante à la stratégie de clé existante.

```
{
```

```
"Sid": "Allow Amazon S3 use of the CMK",
"Effect": "Allow",
"Principal": {
  "Service": "s3.amazonaws.com"
},
"Action": [
  "kms:GenerateDataKey"
],
"Resource": "*"
}
```

9. Sélectionnez Save Changes.

Pour plus d'informations sur la création de CMK gérés par le client AWS KMS et l'utilisation de stratégies clés, consultez les liens suivants dans le AWS Key Management Service Developer Guide:

- [Démarrez](#)
- [Utilisation de stratégies de clé dans AWS KMS](#)

Plus d'informations

[Gestion du stockage \(p. 83\)](#)

## Comment créer un filtre de métriques des demandes pour tous les objets de mon compartiment S3 ?

Il existe trois types de métriques Amazon CloudWatch pour Amazon S3 : les métriques de stockage, les métriques de demande et les métriques de réplication. Les métriques du stockage sont fournies une fois par jour à tous les clients sans frais supplémentaires. Ces métriques des demandes sont disponibles à intervalles d'une minute après une latence de traitement. Ces métriques des demandes sont facturées au tarif standard CloudWatch. Vous devez activer les métriques des demandes dans la console ou en utilisant l'API Amazon S3.

Pour plus d'informations sur les métriques CloudWatch pour Amazon S3, consultez [Surveillance des métriques avec Amazon CloudWatch](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

### Configuration des métriques des demandes pour tous les objets d'un compartiment S3

Pour configurer les métriques des demandes sur un compartiment

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient les objets pour lesquels vous souhaitez les métriques de demande.
3. Choisissez l'onglet Management, puis choisissez Metrics.
4. Choisissez Requêtes.
5. Choisissez l'icône de modification en regard de l'icône de compartiment.
6. Pour créer la configuration des métriques des demandes pour tous les objets de votre compartiment, cochez la case Métriques des demandes.

7. Choisissez Enregistrer.

Après environ 15 minutes, CloudWatch commence à suivre ces métriques des demandes. Vous pouvez voir les graphiques des métriques dans la console CloudWatch ou Amazon S3. Ces métriques des demandes sont facturées au tarif standard CloudWatch. Pour de plus amples informations, consultez [Tarification Amazon CloudWatch](#).

Vous pouvez également créer un filtre qui limite la portée des métriques de réplication par des préfixes ou des balises. Pour de plus amples informations, veuillez consulter [Comment créer un filtre de métriques des demandes qui limite la portée par balise ou préfixe d'objet ?](#) (p. 115)

## Comment créer un filtre de métriques des demandes qui limite la portée par balise ou préfixe d'objet ?

Il existe trois types de métriques Amazon CloudWatch pour Amazon S3 : les métriques de stockage, les métriques de demande et les métriques de réplication. Les métriques du stockage sont fournies une fois par jour à tous les clients sans frais supplémentaires. Ces métriques sont disponibles à intervalles d'une minute après une latence de traitement. Ces métriques des demandes sont facturées au tarif standard CloudWatch. Vous devez activer les métriques des demandes dans la console ou en utilisant l'API Amazon S3.

Pour plus d'informations sur les métriques CloudWatch pour Amazon S3, consultez [Surveillance des métriques avec Amazon CloudWatch](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

### Création d'un filtre de métriques des demandes qui limite la portée par balise ou préfixe d'objet

Pour filtrer les métriques des demandes sur un sous-ensemble d'objets stockés dans un compartiment

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient les objets pour lesquels vous souhaitez les métriques de demande.
3. Choisissez l'onglet Management, puis choisissez Metrics.
4. Choisissez Requêtes.
5. Dans le volet gauche, à côté de Filtres, choisissez Ajouter.
6. Dans Nom du filtre, saisissez un nom pour votre filtre de métriques des demandes.
7. Dans Préfixe/balises que vous souhaitez surveiller, saisissez un préfixe ou une balise, puis choisissez le préfixe ou la balise dans la liste déroulante qui s'affiche.
8. Pour ajouter des balises ou des filtres supplémentaires, répétez l'étape précédente.
9. Choisissez Enregistrer.

Vous avez maintenant créé un filtre qui limite la portée des métriques des demandes par des balises et des préfixes d'objet. Environ 15 minutes après que CloudWatch commence à effectuer le suivi de ces métriques des demandes, vous pouvez afficher les graphiques correspondants à la fois dans les consoles Amazon S3 ou CloudWatch. Ces métriques des demandes sont facturées au tarif standard CloudWatch. Pour de plus amples informations, veuillez consulter [Tarification Amazon CloudWatch](#).



Vous pouvez également configurer les métriques des demandes au niveau d'un compartiment. Pour plus d'informations, consultez [Comment créer un filtre de métriques des demandes pour tous les objets de mon compartiment S3 ?](#) (p. 114)

## Comment supprimer un filtre de métriques des demandes ?

Dans la console Amazon S3, vous pouvez supprimer un filtre de métriques des demandes. Lorsque vous supprimez un filtre, les métriques des demandes qui utilisent ce filtre spécifique ne vous sont plus facturées. Toutefois, vous continuerez à être facturé pour toute autre configuration de filtre existante. Lorsque vous supprimez un filtre, vous ne pouvez plus l'utiliser pour les métriques des demandes. La suppression d'un filtre ne peut pas être annulée.

Pour plus d'informations sur la création d'un filtre de métriques des demandes, consultez [Comment créer un filtre de métriques des demandes pour tous les objets de mon compartiment S3 ?](#) (p. 114) et [Comment créer un filtre de métriques des demandes qui limite la portée par balise ou préfixe d'objet ?](#) (p. 115)

### Suppression d'un filtre de métriques des demandes

Pour supprimer un filtre qui limite la portée avec des balises ou des préfixes

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Compartiment, choisissez le nom du compartiment qui contient les objets pour lesquels vous souhaitez les métriques des demandes.
3. Choisissez l'onglet Management, puis choisissez Metrics.
4. Choisissez Requêtes.
5. Sous Filtres, choisissez l'icône de modification à côté de votre filtre.

Important

La suppression d'un filtre ne peut pas être annulée.

6. Choisissez Delete filter.

Amazon S3 supprime votre filtre.

Supprimer un filtre pour tous les objets de votre compartiment

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Compartiment, choisissez le nom du compartiment qui contient les objets pour lesquels vous souhaitez les métriques des demandes.
3. Choisissez l'onglet Management, puis choisissez Metrics.
4. Choisissez Requêtes.
5. Choisissez l'icône modification à côté de l'icône compartiment.
6. Effacer les métriques des demandes.

L'effacement des métriques des demandes efface également les métriques de transfert de données.

7. Choisissez Save.

## Comment afficher les métriques de réplication ?

Il existe trois types de métriques Amazon CloudWatch pour Amazon S3 : les métriques de stockage, les métriques de demande et les métriques de réplication. Les métriques de réplication sont activées automatiquement lorsque vous activez la réplication avec S3 Replication Time Control (S3 RTC) à l'aide de la AWS Management Console ou de l'API Amazon S3. Les métriques de réplication sont disponibles 15 minutes après l'activation d'une règle de réplication avec S3 Replication Time Control (S3 RTC) (S3 RTC).

Les métriques de réplication suivent les ID de règle de la configuration de réplication. Un ID de règle de réplication peut être spécifique à un préfixe, à une balise ou à une combinaison des deux. Pour plus d'informations sur S3 Replication Time Control (S3 RTC), consultez [Réplication d'objets à l'aide de S3 Replication Time Control \(S3 RTC\)](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Pour plus d'informations sur les métriques CloudWatch pour Amazon S3, consultez [Surveillance des métriques avec Amazon CloudWatch](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

### Affichage des métriques de réplication

#### Prérequis

Activez une règle de réplication qui possède S3 RTC.

Pour afficher les métriques de réplication

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient les objets pour lesquels vous souhaitez les métriques de réplication.
3. Choisissez l'onglet Management, puis choisissez Metrics.
4. Choisissez Réplication.
5. Dans la liste Rule IDs (ID de règle) dans le volet de gauche, sélectionnez les ID de règle de votre choix. Si vous avez à choisir parmi plusieurs ID de règle, vous pouvez rechercher les ID souhaités.
6. Après avoir sélectionné les ID de règle de votre choix, choisissez Display graphs (Afficher les graphiques) sous la zone de sélection Rule IDs (ID de règle).

Vous pouvez ensuite afficher les métriques de réplication Replication Latency (in seconds) (Latence de réplication (en secondes)), Operations pending replication (Opérations en attente de réplication), et Bytes pending replication (Octets en attente de réplication) pour les règles que vous avez sélectionnées. Amazon CloudWatch commence à signaler les métriques de réplication 15 minutes après que vous avez activé S3 RTC sur la règle de réplication respective. Vous pouvez afficher les métriques de réplication sur Amazon S3 ou sur la console CloudWatch. Pour plus d'informations, consultez [Présentation des métriques de réplication](#) dans le Amazon Simple Storage Service Manuel du développeur.

# Définition des autorisations d'accès aux compartiments et aux objets

Cette section explique comment utiliser la console Amazon Simple Storage Service (Amazon S3) pour donner des autorisations d'accès à vos compartiments et à vos objets. Elle explique aussi comment utiliser le blocage d'accès public Amazon S3 pour empêcher l'application de paramètres autorisant un accès public aux données dans des compartiments S3.

Les compartiments et les objets sont des ressources Amazon S3. Les stratégies d'accès basées sur les ressources vous permettent d'accorder des autorisations d'accès aux compartiments et aux objets. Vous pouvez associer une stratégie d'accès à une ressource. Une stratégie d'accès décrit qui a accès aux ressources. Le propriétaire de la ressource est le compte AWS qui l'a créée. Pour plus d'informations sur la propriété des ressources et les stratégies d'accès, consultez [Présentation de la gestion de l'accès](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Les autorisations d'accès aux compartiments vous permettent de spécifier les utilisateurs autorisés à accéder aux objets stockés dans un compartiment et de définir les types d'accès dont ils bénéficient. Les autorisations d'accès aux objets vous permettent de spécifier les utilisateurs autorisés à accéder à l'objet et de définir les types d'accès dont ils bénéficient. Par exemple, vous pouvez accorder seulement une autorisation de lecture à un utilisateur, et des autorisations de lecture et d'écriture à un autre.

Les autorisations de compartiment et d'objet sont indépendantes les unes des autres. un objet n'hérite pas des autorisations de son compartiment. Par exemple, si vous créez un compartiment et accordez un accès en écriture à un utilisateur, vous ne pouvez pas accéder à ses objets sauf s'il vous accorde explicitement l'accès. Les autorisations de compartiment permettent généralement à un utilisateur de répertorier des informations sur un compartiment, et d'ajouter des objets à un compartiment, ainsi que de supprimer des objets d'un compartiment. Les autorisations d'objet permettent généralement à un utilisateur de télécharger, remplacer ou supprimer des objets.

## Note

Vous n'avez pas nécessairement besoin d'accorder des autorisations de compartiment pour accorder des autorisations d'objet, et vice versa. Par exemple, vous pouvez utiliser la console AWS pour accorder à un utilisateur des autorisations de mise à jour sur un objet sans accorder à cet utilisateur des autorisations pour le compartiment contenant cet objet. Toutefois, si vous n'accordez des autorisations qu'à l'objet, et non au compartiment, le bénéficiaire ne sera pas en mesure d'utiliser la console AWS pour accéder à l'objet. (Il ne sera pas en mesure d'afficher l'objet dans la console, car il ne sera pas en mesure d'afficher le compartiment contenant l'objet.) Le bénéficiaire devra alors accéder à l'objet par programme, par exemple avec l'interface de ligne de commande AWS.

Pour accorder à d'autres comptes AWS et au grand public un accès à vos compartiments et objets, vous utilisez les stratégies d'accès basées sur les ressources nommées listes de contrôle d'accès (ACL).

Une stratégie de compartiment est une stratégie AWS Identity and Access Management (IAM) basée sur les ressources qui accorde à d'autres comptes AWS ou utilisateurs IAM un accès à un compartiment S3. Les stratégies de compartiment complètent, et dans de nombreux cas, remplacent les stratégies d'accès basées sur les listes ACL. Pour plus d'informations sur l'utilisation d'IAM avec Amazon S3, consultez [Gestion des autorisations d'accès de vos ressources Amazon S3](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Pour des informations plus complètes sur la gestion des autorisations d'accès, consultez [Présentation de la gestion des autorisations d'accès aux ressources Amazon S3](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Cette section explique également comment utiliser la console Amazon S3 pour ajouter une configuration CORS (partage des ressources cross-origine) à un compartiment S3. La spécification CORS permet aux applications Web clientes chargées dans un domaine particulier d'interagir avec les ressources d'un autre domaine.

#### Rubriques

- [Comment bloquer l'accès public à des compartiments S3 ? \(p. 119\)](#)
- [Comment modifier les paramètres d'accès public pour des compartiments S3 ? \(p. 120\)](#)
- [Comment modifier les paramètres d'accès public pour tous les compartiments S3 d'un compte AWS ? \(p. 123\)](#)
- [Comment définir les autorisations d'un objet ? \(p. 124\)](#)
- [Comment définir des autorisations de compartiment ACL ? \(p. 127\)](#)
- [Comment ajouter une stratégie de compartiment S3 ? \(p. 131\)](#)
- [Comment ajouter le partage des ressources inter-domaines avec le partage CORS ? \(p. 132\)](#)
- [Définir S3 Propriété de l'objet sur le propriétaire du compartiment préféré dans la AWS Management Console \(p. 134\)](#)
- [Utiliser Access Analyzer for S3 \(p. 134\)](#)

## Comment bloquer l'accès public à des compartiments S3 ?

Le blocage de l'accès public Amazon S3 empêche l'application de paramètres qui autorisent un accès public aux données dans des compartiments S3. Vous pouvez configurer les paramètres de blocage d'accès public pour des compartiments S3 individuels ou tous les compartiments votre compte. Pour plus d'informations sur le blocage de l'accès public à l'aide de l'AWS CLI, des kits SDK AWS et des API REST Amazon S3, consultez [Utilisation du blocage d'accès public Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

Les rubriques suivantes expliquent comment utiliser la console Amazon S3 pour configurer les paramètres de blocage d'accès public :

- [Comment modifier les paramètres d'accès public pour des compartiments S3 ? \(p. 120\)](#)
- [Comment modifier les paramètres d'accès public pour tous les compartiments S3 d'un compte AWS ? \(p. 123\)](#)

Les sections suivantes expliquent comment afficher le statut d'accès d'un compartiment et effectuer une recherche par type d'accès.

## Affichage du statut d'accès

La vue de liste de compartiments montre si un compartiment est accessible publiquement. Amazon S3 étiquette les autorisations pour un compartiment comme suit :

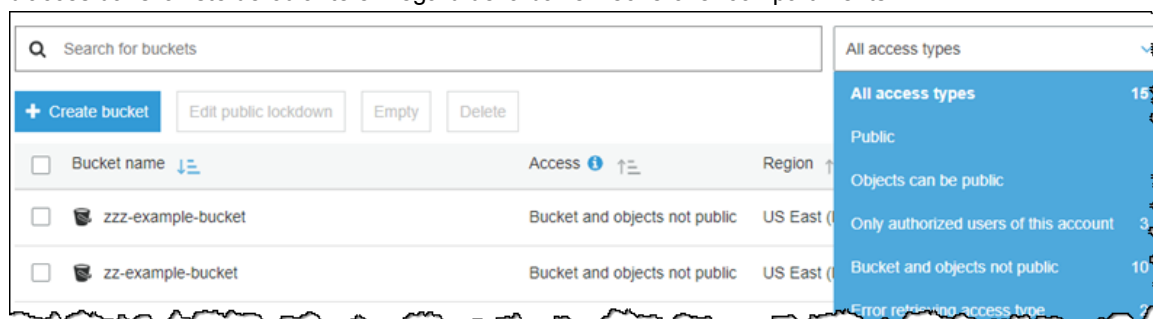
- Public – N'importe qui a accès à une ou plusieurs des autorisations suivantes : Lister les objets, Écrire les objets, autorisations en lecture et écriture.
- Les objets peuvent être publics – Le compartiment n'est pas public, mais toute personne avec les autorisations appropriées peut accorder l'accès public à des objets.
- Compartiments et objets non publics – Le compartiment et les objets n'ont aucun accès public.

- Seuls les utilisateurs autorisés de ce compte – L'accès est limité aux utilisateurs et rôles IAM de ce compte, et aux mandataires de service AWS, car une stratégie accorde l'accès public.

La colonne d'accès affiche le statut d'accès des compartiments répertoriés.

<input type="checkbox"/> Bucket name	Access	Region
<input type="checkbox"/> zzz-example-bucket	Bucket and objects not public	US East (N. Virginia)
<input type="checkbox"/> zz-example-bucket	Only authorized users of this account	US East (N. Virginia)
<input type="checkbox"/> example-bucket-77	Error	US East (N. Virginia)

Vous pouvez également filtrer les recherches de compartiment par type d'accès. Choisissez un type d'accès dans la liste déroulante en regard de la barre Rechercher compartiments.



## Plus d'informations

- [Comment modifier les paramètres d'accès public pour des compartiments S3 ? \(p. 120\)](#)
- [Comment modifier les paramètres d'accès public pour tous les compartiments S3 d'un compte AWS ? \(p. 123\)](#)
- [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#)
- [Restriction de l'accès à l'aide d'une identité d'accès à l'origine](#) dans le Amazon Simple Storage Service Manuel du développeur
- [Accès au contenu privé dans Amazon CloudFront](#) dans le Blog des développeurs AWS

## Comment modifier les paramètres d'accès public pour des compartiments S3 ?

La fonction Amazon S3 Block Public Access empêche l'application de paramètres qui autorisent un accès public aux données dans des compartiments S3. Cette section explique comment modifier les paramètres Block Public Access pour un ou plusieurs compartiments S3. Pour plus d'informations sur le blocage de l'accès public à l'aide de l'AWS CLI, des kits SDK AWS et des API REST Amazon S3, consultez [Utilisation du blocage d'accès public Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

### Rubriques

- [Modification des paramètres d'accès public pour un compartiment S3 \(p. 121\)](#)
- [Modification des paramètres d'accès public pour plusieurs compartiments S3 \(p. 121\)](#)

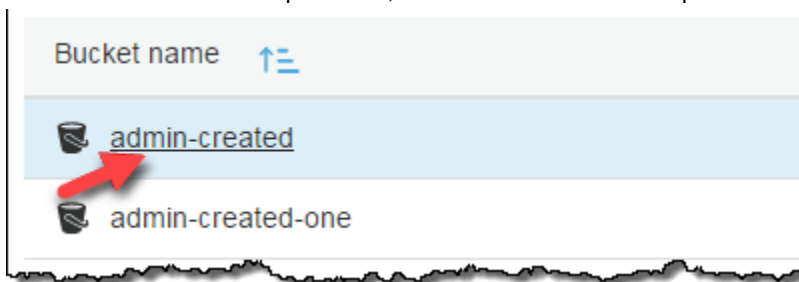
- [Plus d'informations \(p. 122\)](#)

## Modification des paramètres d'accès public pour un compartiment S3

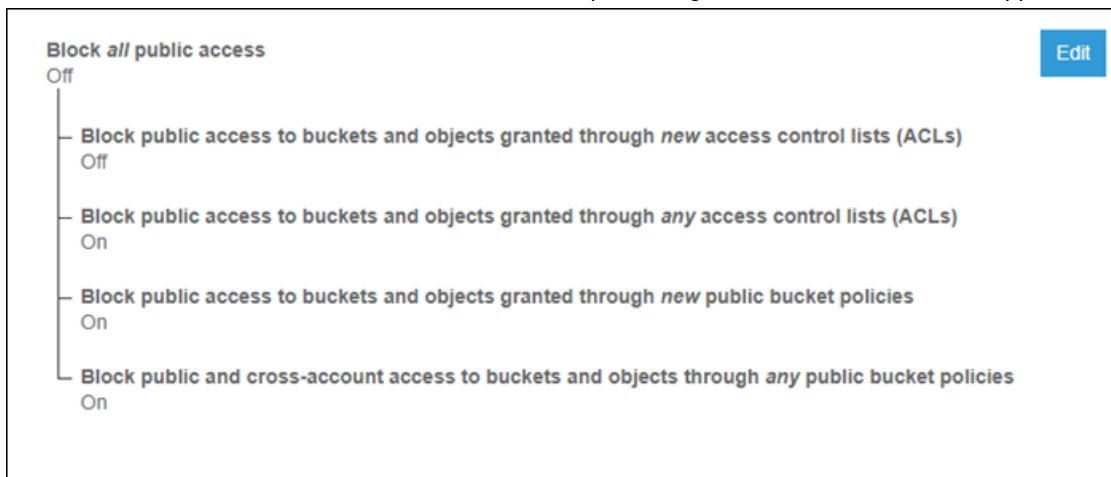
Suivez ces étapes si vous devez modifier les paramètres d'accès public pour un seul compartiment S3.

Pour modifier les paramètres Amazon S3 Block Public Access pour un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment.



3. Choisissez Autorisations.
4. Choisissez Modifier pour modifier les paramètres d'accès public pour le compartiment. Pour de plus amples informations sur les quatre paramètres Amazon S3 Block Public Access, veuillez consulter [Paramètres Block Public Access](#) dans le Amazon Simple Storage Service Manuel du développeur.



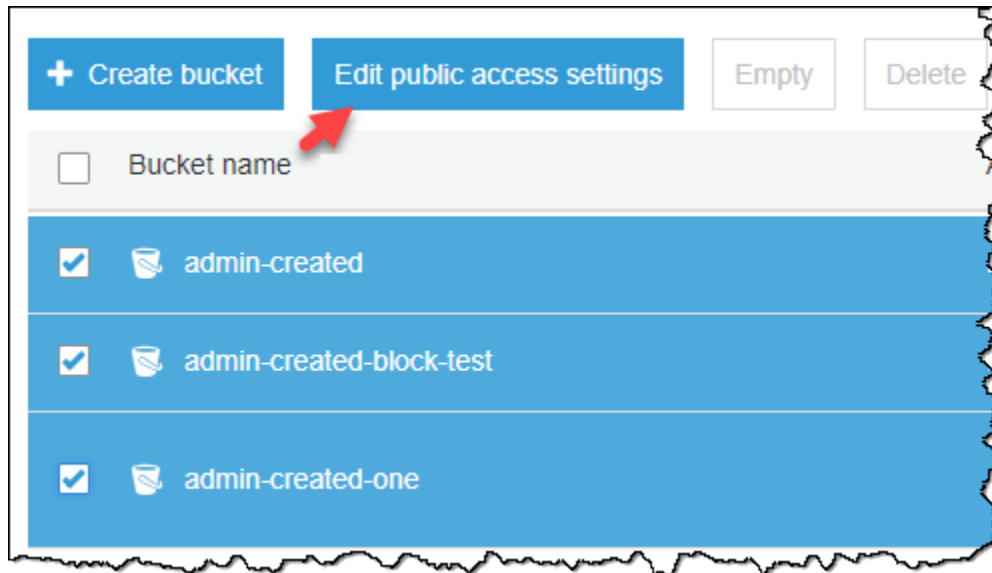
5. Choisissez le paramètre que vous souhaitez modifier, puis Enregistrer.
6. Lorsque vous êtes invité à confirmer l'opération, entrez **confirm**. Choisissez ensuite Confirmer pour enregistrer vos modifications.

## Modification des paramètres d'accès public pour plusieurs compartiments S3

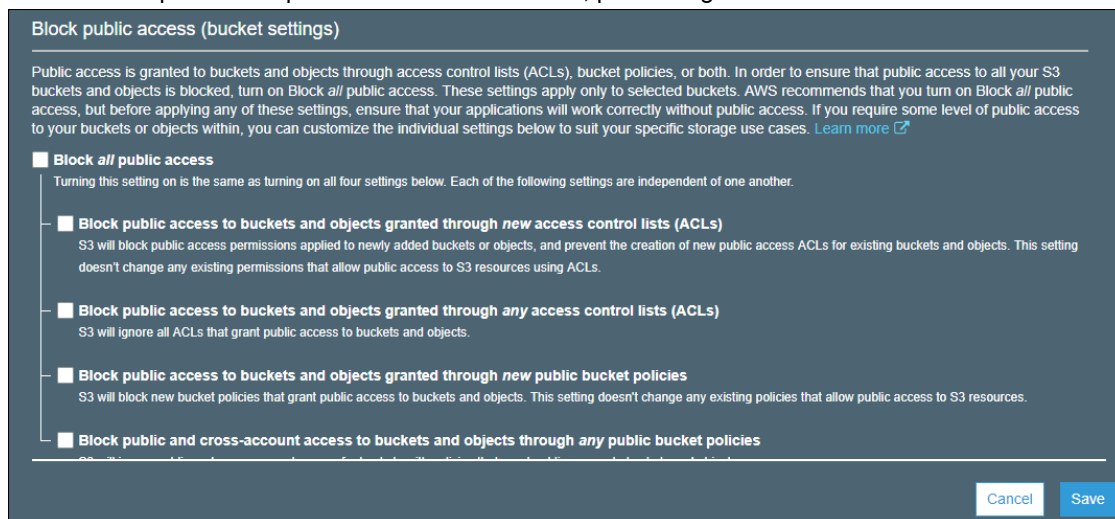
Suivez ces étapes si vous devez modifier les paramètres d'accès public pour plusieurs compartiments S3.

Pour modifier les paramètres Amazon S3 Block Public Access pour plusieurs compartiments S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez les compartiments souhaités, puis Edit public access settings (Modifier les paramètres d'accès public).



3. Choisissez le paramètre que vous souhaitez modifier, puis Enregistrer.



4. Lorsque vous êtes invité à confirmer l'opération, entrez **confirm**. Choisissez ensuite Confirmer pour enregistrer vos modifications.

Vous pouvez modifier les paramètres Amazon S3 Block Public Access suivants lorsque vous créez un compartiment. Pour de plus amples informations, veuillez consulter [Comment créer un compartiment S3 ? \(p. 4\)](#).

## Plus d'informations

- [Comment bloquer l'accès public à des compartiments S3 ? \(p. 119\)](#)

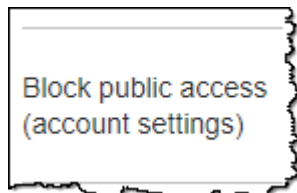
- [Comment modifier les paramètres d'accès public pour tous les compartiments S3 d'un compte AWS ? \(p. 123\)](#)
- [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#)

## Comment modifier les paramètres d'accès public pour tous les compartiments S3 d'un compte AWS ?

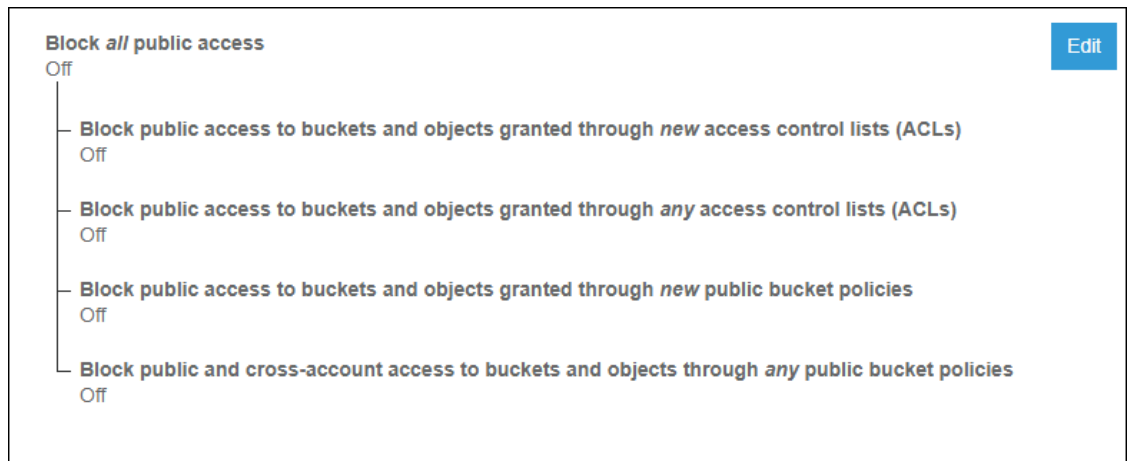
Le blocage de l'accès public Amazon S3 empêche l'application de paramètres qui autorisent un accès public aux données dans des compartiments S3. Cette section explique comment modifier les paramètres de blocage d'accès public pour tous les compartiments S3 de votre compte AWS. Pour plus d'informations sur le blocage de l'accès public à l'aide de l'AWS CLI, des kits SDK AWS et des API REST Amazon S3, consultez [Utilisation du blocage d'accès public Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour modifier les paramètres de blocage d'accès public pour tous les compartiments S3 d'un compte AWS

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Choisissez Block Public Access (paramètres du compte).



3. Choisissez Modifier pour modifier les paramètres de blocage d'accès public pour tous les compartiments de votre compte AWS.



4. Choisissez les paramètres que vous souhaitez modifier, puis Save (Enregistrer).
5. Lorsque vous êtes invité à confirmer l'opération, entrez **confirm**. Choisissez ensuite Confirmer pour enregistrer vos modifications.

## Plus d'informations

- [Comment bloquer l'accès public à des compartiments S3 ? \(p. 119\)](#)



- [Comment modifier les paramètres d'accès public pour des compartiments S3 ? \(p. 120\)](#)
- [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#)

## Comment définir les autorisations d'un objet ?

Cette section explique comment utiliser la console Amazon Simple Storage Service (Amazon S3) pour gérer les autorisations d'accès d'un objet Amazon S3 à l'aide des listes de contrôle d'accès (ACL). Les listes de contrôle d'accès sont des stratégies d'accès basées sur les ressources qui accordent des autorisations d'accès aux compartiments et aux objets. Pour plus d'informations sur la gestion des autorisations d'accès à l'aide des stratégies basées sur les ressources, consultez [Présentation de la gestion de l'accès](#) dans le Amazon Simple Storage Service Manuel du développeur.

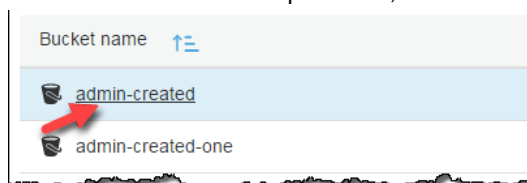
Les autorisations de compartiment et d'objet sont indépendantes les unes des autres. un objet n'hérite pas des autorisations de son compartiment. Par exemple, si vous créez un compartiment et accordez un accès en écriture à un utilisateur, vous ne pouvez pas accéder à ses objets sauf s'il vous accorde explicitement l'accès.

Vous pouvez accorder des autorisations à d'autres comptes AWS ou à des groupes prédéfinis. L'utilisateur ou le groupe auquel vous accordez des autorisations est le « bénéficiaire ». Par défaut, le propriétaire, c'est-à-dire le compte AWS qui a créé le compartiment, dispose des autorisations complètes.

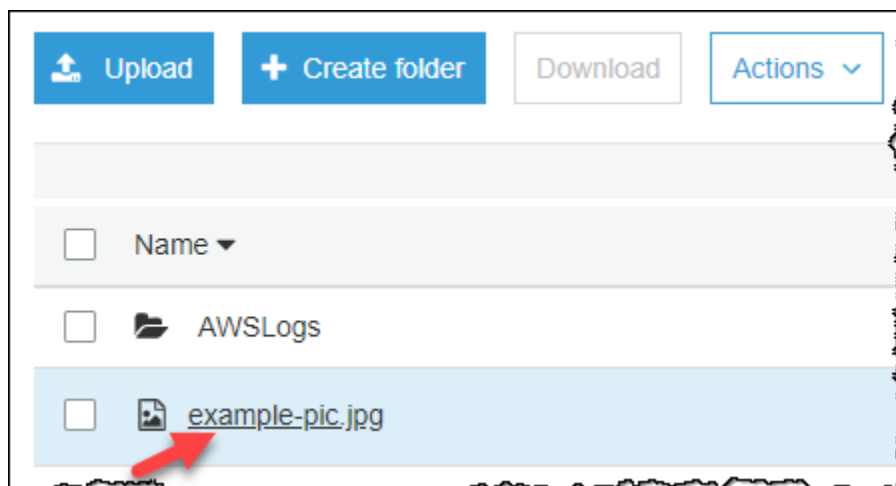
Chaque autorisation accordée pour un utilisateur ou un groupe ajoute une entrée dans la liste ACL associée à l'objet. Les listes ACL répertorient le bénéficiaire et l'autorisation accordée. Pour plus d'informations sur les listes de contrôle d'accès, consultez [Gestion des accès avec les listes ACL](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

Pour définir des autorisations pour un objet

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment qui contient l'objet.



3. Dans la liste Name (Nom), sélectionnez le nom de l'objet pour lequel vous souhaitez définir des autorisations.

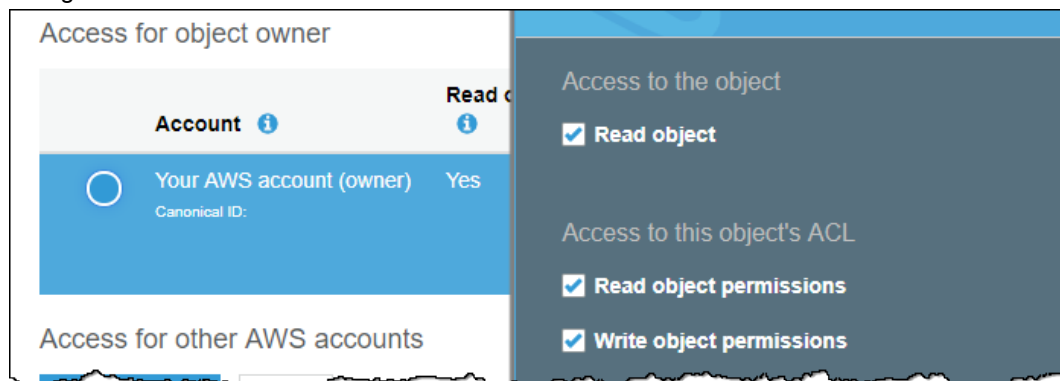


4. Choisissez Autorisations.
5. Vous pouvez gérer les autorisations d'accès aux objets pour :
  - a. Accès pour le propriétaire de l'objet

Le propriétaire désigne l'utilisateur racine du compte AWS et non un utilisateur AWS Identity and Access Management (IAM). Pour en savoir plus sur l'utilisateur racine, consultez [Utilisateur racine d'un compte AWS](#) dans le IAM Guide de l'utilisateur.

Pour modifier les autorisations d'accès à l'objet du propriétaire, sous Accès pour le propriétaire de l'objet, choisissez Votre compte AWS (propriétaire).

Activez les cases à cocher des autorisations que vous souhaitez modifier, puis choisissez Enregistrer.



- b. Modalités d'accès pour les autres comptes AWS

Pour accorder des autorisations à un utilisateur AWS d'un autre compte AWS, sous Accès pour d'autres comptes AWS, choisissez Ajouter un compte. Dans le champ Saisir un ID, tapez l'ID canonique de l'utilisateur AWS auquel vous souhaitez accorder des autorisations relatives à un objet. Pour en savoir plus sur la recherche d'un ID canonique, consultez [Identificateurs de compte AWS](#) dans le Référence générale d'Amazon Web Services. Vous pouvez ajouter jusqu'à 99 utilisateurs.

Activez les cases à cocher des autorisations que vous souhaitez accorder à l'utilisateur, puis choisissez Enregistrer. Pour afficher des informations sur les autorisations, choisissez les icônes d'aide.

Account	Read object
79a59df900b949e55d96a1e698fbac...	<input checked="" type="checkbox"/> Yes

c. Accès public

Pour permettre au grand public (tout le monde) d'accéder à votre objet, sous Accès public, sélectionnez Tout le monde. Si vous accordez des autorisations d'accès public, tout le monde peut accéder à l'objet.

Activez les cases à cocher des autorisations que vous souhaitez accorder, puis choisissez Enregistrer.

**Everyone**

**Warning:** This object will have public access. Everyone will have access to one or all of the following: read this object, read and write permissions.

Access to the object

☒ Read object

Access to this object's ACL

☐ Read object permissions

☐ Write object permissions

Cancel Save

Warning

- Soyez vigilant lorsque vous accordez au groupe Tout le monde l'accès anonyme à vos objets Amazon S3. Lorsque vous accordez l'accès à ce groupe, tout le monde peut accéder à votre

objet. Si vous avez besoin d'accorder l'accès à tout le monde, nous vous recommandons vivement d'octroyer uniquement des autorisations Lecture d'objet.

- Nous vous recommandons de ne pas accorder des autorisations d'écriture sur l'objet au groupe Tout le monde. Si vous le faites, n'importe qui peut remplacer les autorisations de liste ACL pour l'objet.

#### Note

Cette action applique des autorisations à tous les objets spécifiés. Lors de l'application des autorisations à des dossiers, attendez la fin de l'opération d'enregistrement pour ajouter de nouveaux objets.

Vous pouvez également définir des autorisations pour les objets lorsque vous chargez ces derniers. Pour plus d'informations sur la définition des autorisations lors du chargement des objets, consultez [Comment charger des fichiers ou des dossiers dans un compartiment S3 ? \(p. 37\)](#).

## Plus d'informations

- [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#)
- [Comment définir des autorisations de compartiment ACL ? \(p. 127\)](#)

## Comment définir des autorisations de compartiment ACL ?

Cette section explique comment utiliser la console Amazon Simple Storage Service (Amazon S3) pour gérer les autorisations d'accès des compartiments S3 à l'aide des listes de contrôle d'accès (ACL). Les listes de contrôle d'accès sont des stratégies d'accès basées sur les ressources qui accordent des autorisations d'accès aux compartiments et aux objets. Pour plus d'informations sur la gestion des autorisations d'accès à l'aide des stratégies basées sur les ressources, consultez [Présentation de la gestion de l'accès](#) dans le Amazon Simple Storage Service Manuel du développeur.

Vous pouvez accorder des autorisations à d'autres utilisateurs de comptes AWS ou à des groupes prédéfinis. L'utilisateur ou le groupe auquel vous accordez des autorisations est le « bénéficiaire ». Par défaut, le propriétaire, c'est-à-dire le compte AWS qui a créé le compartiment, dispose des autorisations complètes.

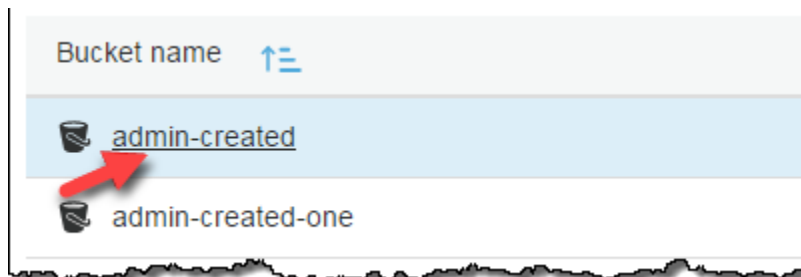
Chaque autorisation accordée pour un utilisateur ou un groupe ajoute une entrée dans la liste ACL associée au compartiment. Les listes ACL répertorient le bénéficiaire et l'autorisation accordée. Pour plus d'informations sur les listes de contrôle d'accès, consultez [Gestion des accès avec les listes ACL](#) dans le manuel Amazon Simple Storage Service Manuel du développeur.

#### Warning

Nous vous recommandons fortement d'éviter d'accorder l'accès en écriture aux groupes Tout le monde (accès public) ou Groupe d'utilisateurs authentifiés (tous les utilisateurs authentifiés AWS). Pour plus d'informations sur les effets de l'octroi d'un accès en écriture à ces groupes, consultez [Groupes prédéfinis Amazon S3](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour définir des autorisations d'accès ACL pour un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez définir des autorisations.

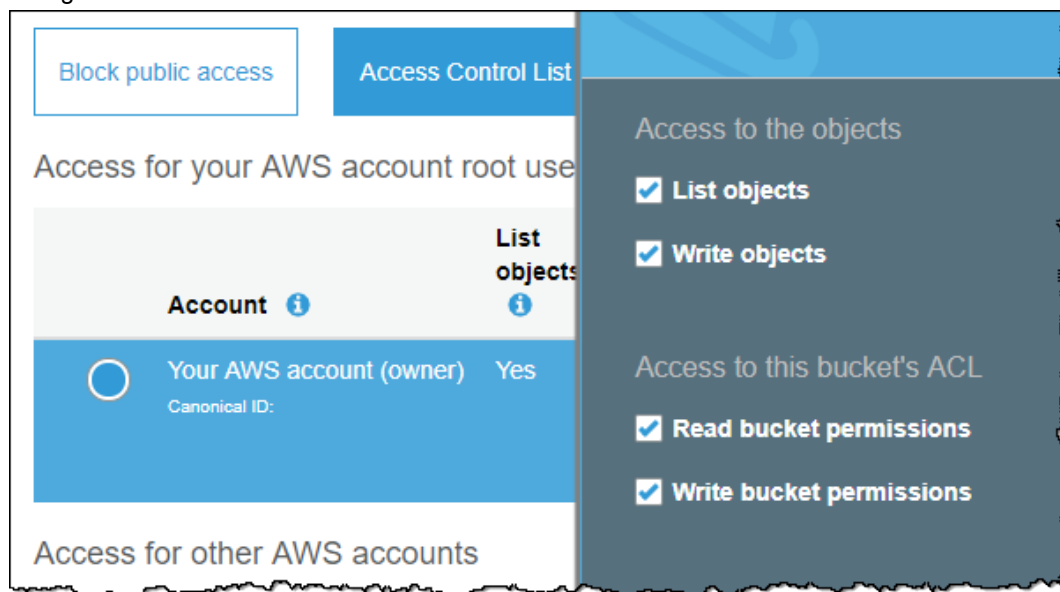


3. Sélectionnez Autorisations, puis choisissez Liste de contrôle d'accès.
4. Vous pouvez gérer les autorisations d'accès aux compartiments :
  - a. Accès de l'utilisateur racine de votre compte AWS

Le propriétaire désigne l'utilisateur racine du compte AWS et non un utilisateur AWS Identity and Access Management (IAM). Pour en savoir plus sur l'utilisateur racine, consultez [Utilisateur racine d'un compte AWS](#) dans le IAM Guide de l'utilisateur.

Pour modifier les autorisations d'accès au compartiment du propriétaire, sous Accès de l'utilisateur racine de votre compte AWS, choisissez Votre compte AWS (propriétaire).

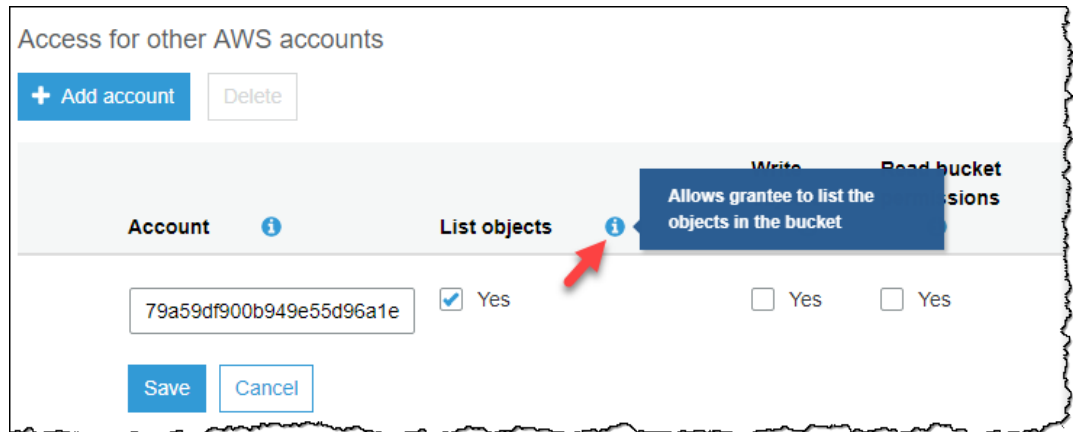
Activez les cases à cocher des autorisations que vous souhaitez modifier, puis choisissez Enregistrer.



- b. Modalités d'accès pour les autres comptes AWS

Pour accorder des autorisations à un utilisateur AWS d'un autre compte AWS, sous Accès pour d'autres comptes AWS, choisissez Ajouter un compte. Dans le champ Saisir un ID, tapez l'ID canonique de l'utilisateur AWS auquel vous souhaitez accorder des autorisations relatives à un compartiment. Pour en savoir plus sur la recherche d'un ID canonique, consultez [Identificateurs de compte AWS](#) dans le Référence générale d'Amazon Web Services. Vous pouvez ajouter jusqu'à 99 utilisateurs.

Activez les cases à cocher en regard des autorisations que vous souhaitez accorder à l'utilisateur, puis choisissez Enregistrer. Pour afficher des informations sur les autorisations, choisissez les icônes d'aide.



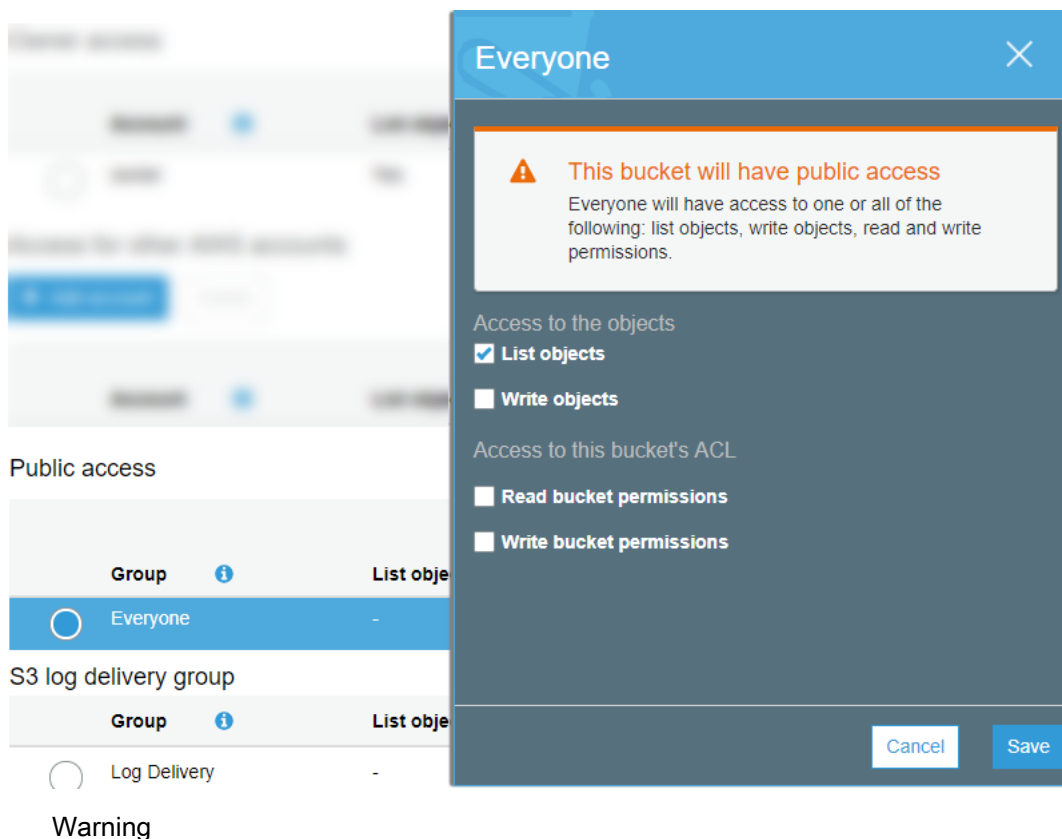
#### Warning

Lorsque vous accordez à d'autres comptes AWS l'accès aux ressources, sachez que les comptes AWS peuvent déléguer leurs autorisations aux utilisateurs sous leurs comptes. Il s'agit d'un accès entre comptes. Pour en savoir plus sur l'utilisation de l'accès entre comptes, consultez [Création d'un rôle pour déléguer des autorisations à un utilisateur IAM](#) dans le IAM Guide de l'utilisateur.

#### c. Accès public

Pour permettre au grand public (n'importe qui dans le monde) d'accéder à votre compartiment, sous Accès public, sélectionnez Tout le monde. Si vous accordez des autorisations d'accès public, tout le monde peut accéder au compartiment. Activez les cases à cocher des autorisations que vous souhaitez accorder, puis choisissez Enregistrer.

Pour ne plus permettre au public d'accéder à votre compartiment, sélectionnez Tout le monde sous Accès public. Désélectionnez toutes les cases d'autorisations, puis choisissez Enregistrer.



Soyez vigilant lorsque vous accordez au groupe Tout le monde l'accès public à votre compartiment S3. Lorsque vous accordez l'accès à ce groupe, tout le monde peut accéder à votre compartiment. Nous vous recommandons vivement de ne jamais accorder un type d'accès en écriture public quel qu'il soit à votre compartiment S3.

d. Groupe de livraison des journaux S3

Pour permettre à Amazon S3 d'enregistrer des journaux d'accès au serveur dans le compartiment, sous Groupe de livraison des journaux S3, choisissez Livraison des journaux.

Si un compartiment est configuré en tant que compartiment cible (les journaux d'accès y seront stockés), les autorisations sur ce compartiment doivent autoriser le groupe Livraison des journaux à disposer d'un accès en écriture sur le compartiment. Lorsque vous activez la journalisation des accès serveur sur un compartiment, la console Amazon S3 accorde au groupe Livraison des journaux un droit d'accès en écriture sur le compartiment cible que vous avez choisi pour la réception des journaux. Pour en savoir plus sur la journalisation des accès au serveur, consultez [Comment activer la journalisation des accès au serveur pour un compartiment S3 ? \(p. 13\)](#).

Vous pouvez également définir des autorisations sur un compartiment lors de la création de ce dernier. Pour en savoir plus sur la définition des autorisations lors de la création d'un compartiment, consultez [Comment créer un compartiment S3 ? \(p. 4\)](#).

## Plus d'informations

- [Définition des autorisations d'accès aux compartiments et aux objets \(p. 118\)](#)
- [Comment définir les autorisations d'un objet ? \(p. 124\)](#)
- [Comment ajouter une stratégie de compartiment S3 ? \(p. 131\)](#)

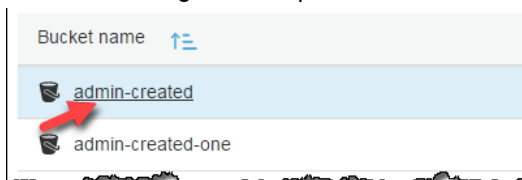
## Comment ajouter une stratégie de compartiment S3 ?

Cette section explique comment utiliser la console Amazon Simple Storage Service (Amazon S3) pour ajouter une stratégie de compartiment ou modifier une stratégie de compartiment existante. Une stratégie de compartiment est une stratégie AWS Identity and Access Management (IAM) basée sur les ressources. Vous ajoutez une stratégie de compartiment à un compartiment pour attribuer à d'autres comptes AWS ou à des utilisateurs IAM des autorisations d'accès pour le compartiment et les objets qu'il contient. Les autorisations d'objets ne s'appliquent qu'aux objets créés par le propriétaire du compartiment. Pour plus d'informations sur les stratégies de compartiment, consultez [Présentation de la gestion de l'accès](#) dans le Amazon Simple Storage Service Manuel du développeur.

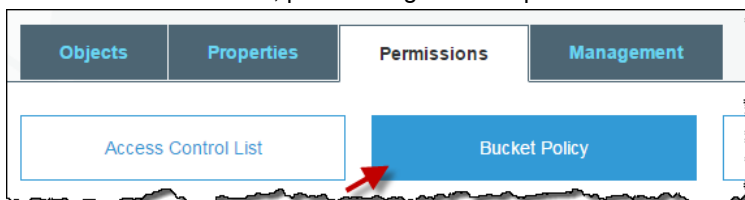
Pour obtenir des exemples de stratégies de compartiment Amazon S3, consultez [Exemples de stratégies de compartiment](#) dans le Amazon Simple Storage Service Manuel du développeur.

Pour créer ou modifier une stratégie de compartiment

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez créer une stratégie de compartiment ou modifier la stratégie de compartiment existante.

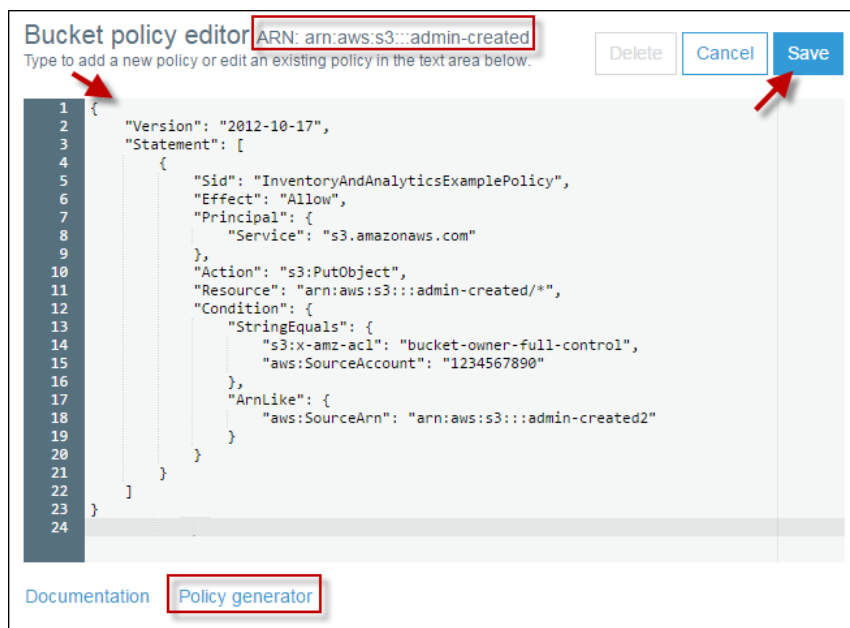


3. Choisissez Autorisations, puis Stratégie de compartiment.



4. Dans la zone Editeur de stratégie de compartiment, tapez ou copiez et collez une nouvelle stratégie de compartiment, ou modifiez une stratégie existante. La stratégie de compartiment est un fichier JSON. Le texte saisi dans l'éditeur doit être une chaîne JSON valide.





5. Choisissez Save.

#### Note

Amazon S3 affiche l'Amazon Resource Name (ARN) du compartiment en regard du titre Editeur de stratégie de compartiment. Pour plus d'informations sur les ARN, consultez [Noms ARN \(Amazon Resource Name\) et espaces de noms du service AWS](#) dans le manuel Référence générale d'Amazon Web Services.

Juste en dessous de la zone de texte de l'éditeur de stratégie de compartiment, vous trouverez un lien vers le Générateur de stratégies, que vous pouvez utiliser pour créer une stratégie de compartiment.

## Plus d'informations

- [Définition des autorisations d'accès aux compartiments et aux objets](#) (p. 118)
- [Comment définir des autorisations de compartiment ACL ?](#) (p. 127)

## Comment ajouter le partage des ressources inter-domaines avec le partage CORS ?

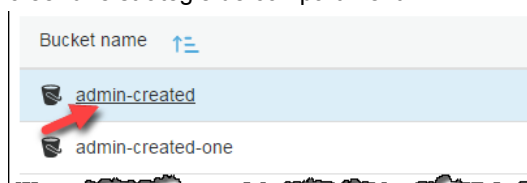
Cette section explique comment utiliser la console Amazon S3 pour ajouter une configuration CORS (partage des ressources cross-origine) à un compartiment S3. La spécification CORS permet aux applications Web clientes chargées dans un domaine particulier d'interagir avec les ressources d'un autre domaine.

Pour configurer le compartiment afin d'autoriser les demandes cross-origine, vous ajoutez la configuration CORS au compartiment. Une configuration CORS est un document XML qui définit les règles identifiant les origines auxquelles vous autorisez l'accès au compartiment, les opérations (méthodes HTTP) prises en charge pour chaque origine, et d'autres informations propres aux opérations. Pour plus d'informations et quelques exemples sur CORS, consultez [Partage des ressources cross-origine \(CORS\)](#) dans le Amazon Simple Storage Service Manuel du développeur.

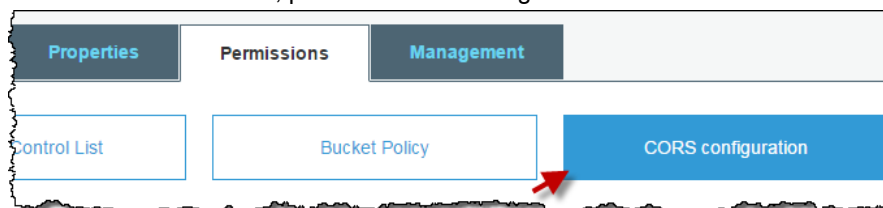
Lorsque vous activez CORS sur le compartiment, les listes de contrôle d'accès (ACL) et les autres stratégies d'autorisation d'accès continuent à s'appliquer.

Pour ajouter une configuration CORS à un compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez créer une stratégie de compartiment.



3. Choisissez Autorisations, puis choisissez Configuration CORS.



4. Dans la zone de texte Editeur de configuration CORS, tapez ou copiez et collez une nouvelle configuration CORS, ou modifiez une configuration existante. La configuration CORS est un fichier XML. Le texte que vous saisissez dans l'éditeur doit être une chaîne XML valide. Pour de plus amples informations, veuillez consulter [Comment configurer le CORS sur un compartiment ?](#)
5. Choisissez Enregistrer.

#### Note

Amazon S3 affiche l'Amazon Resource Name (ARN) du compartiment en regard du titre Editeur de configuration CORS. Pour plus d'informations sur les ARN, consultez [Noms ARN \(Amazon Resource Name\) et espaces de noms du service AWS](#) dans le manuel Référence générale d'Amazon Web Services.

## Plus d'informations

- [Définition des autorisations d'accès aux compartiments et aux objets](#) (p. 118)
- [Comment définir des autorisations de compartiment ACL ?](#) (p. 127)
- [Comment ajouter une stratégie de compartiment S3 ?](#) (p. 131)

## Définir S3 Propriété de l'objet sur le propriétaire du compartiment préféré dans la AWS Management Console

S3 Propriété de l'objet est actuellement en version préalable et peut être configuré via la AWS Management Console, l'AWS Command Line Interface, les kits SDK AWS ou les API REST Amazon S3. La prise en charge de AWS CloudFormation est prévu pour une disponibilité générale.

S3 Propriété de l'objet vous permet de prendre possession des nouveaux objets que d'autres comptes AWS chargent dans votre compartiment avec la liste de contrôle d'accès (ACL) `bucket-owner-full-control` prête à l'emploi. Cette section décrit comment définir Propriété de l'objet à l'aide de la console.

Définir Propriété de l'objet sur le propriétaire du compartiment préféré dans le compartiment S3

1. Connectez-vous à AWS Management Console et ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans la liste Nom du compartiment, choisissez le nom du compartiment pour lequel vous souhaitez activer S3 Propriété de l'objet.
3. Choisissez l'onglet Autorisations.
4. Choisissez S3 Propriété de l'objet.
5. Choisissez Propriétaire du compartiment préféré, puis choisissez Enregistrer.

### Comment puis-je m'assurer que je suis propriétaire des nouveaux objets ?

Avec les étapes ci-dessus, Propriété de l'objet prendra possession de tous les nouveaux objets qui sont écrits par d'autres comptes avec la liste ACL `bucket-owner-full-control` prête à l'emploi. Pour plus d'informations sur l'application d'Propriété de l'objet, consultez [Comment m'assurer que je suis propriétaire des nouveaux objets ?](#) dans le Amazon Simple Storage Service Manuel du développeur.

## Utiliser Access Analyzer for S3

Access Analyzer for S3 vous signale les compartiments S3 configurés pour autoriser l'accès à toute personne sur Internet ou à d'autres comptes AWS, y compris les comptes AWS en dehors de votre entreprise. Pour chaque compartiment public ou partagé, vous recevez des résultats portant sur la source et le niveau des accès public ou partagé. Par exemple, Access Analyzer for S3 peut montrer qu'un compartiment dispose d'un accès en lecture ou en écriture fourni via une liste de contrôle d'accès (ACL) au compartiment, une stratégie de compartiment ou une stratégie de point d'accès. Grâce à ces connaissances, vous pouvez prendre des mesures correctives immédiates et précises pour rétablir l'accès à votre compartiment conformément à vos souhaits originaux.

Lorsque vous examinez un compartiment à risque dans Access Analyzer for S3, vous pouvez bloquer tout accès public au compartiment en un seul clic. Nous vous recommandons de bloquer tous les accès à vos compartiments, sauf si vous avez besoin d'un accès public pour prendre en charge un cas d'utilisation spécifique. Avant de bloquer tout accès public, assurez-vous que vos applications continueront

à fonctionner correctement sans accès public. Pour plus d'informations, consultez [Utilisation d'Amazon S3 Block Public Access](#) dans le Amazon Simple Storage Service Manuel du développeur.

Vous pouvez également aller plus loin en configurant des niveaux d'accès précis dans les paramètres des niveaux d'autorisation des compartiments. Pour des cas d'utilisation spécifiques et vérifiés nécessitant un accès public, tels que l'hébergement statique de site web, les téléchargements publics ou le partage entre comptes, vous pouvez confirmer et enregistrer votre intention pour que le compartiment reste public ou partagé en archivant les résultats du compartiment. Vous pouvez revisiter et modifier ces configurations de compartiments à tout moment. Vous pouvez également télécharger vos résultats sous forme de rapport CSV à des fins d'audit.

Access Analyzer for S3 est disponible gratuitement sur la console Amazon S3. Access Analyzer for S3 est optimisé par AWS Identity and Access Management (IAM) Access Analyzer. Pour l'utiliser Access Analyzer for S3 dans la console Amazon S3, vous devez visiter la console IAM et activer IAM Access Analyzer par région.

Pour plus d'informations sur IAM Access Analyzer, consultez [Qu'est-ce qu'Access Analyzer ?](#) dans le IAM Guide de l'utilisateur. Pour plus d'informations sur Access Analyzer for S3, consultez les sections suivantes.

#### Important

- Access Analyzer for S3 nécessite un analyseur au niveau du compte. Pour utiliser Access Analyzer for S3, vous devez visiter IAM Access Analyzer et créer un analyseur qui a un compte comme zone de confiance. Pour plus d'informations, consultez [Activation de Access Analyzer](#) dans IAM Guide de l'utilisateur.
- Lorsqu'une stratégie de compartiment ou une liste de contrôle d'accès (ACL) de compartiment est ajoutée ou modifiée, Access Analyzer génère et met à jour les résultats en fonction de la modification sous 30 minutes. Il peut s'écouler jusqu'à 6 heures avant que les résultats relatifs aux paramètres de blocage d'accès public au niveau du compte ne soient générés ou mis à jour après la modification des paramètres.

#### Rubriques

- [Quelles sont les informations fournies par Access Analyzer for S3 ? \(p. 135\)](#)
- [Activation d'Access Analyzer for S3 \(p. 136\)](#)
- [Blocage de tous les accès publics \(p. 136\)](#)
- [Vérification et modification de l'accès à un compartiment \(p. 137\)](#)
- [Archivage des résultats de compartiment \(p. 138\)](#)
- [Activation d'un résultat de compartiment archivé \(p. 139\)](#)
- [Affichage des détails de résultats \(p. 139\)](#)
- [Téléchargement d'un rapport Access Analyzer for S3 \(p. 139\)](#)

## Quelles sont les informations fournies par Access Analyzer for S3 ?

Access Analyzer for S3 fournit les résultats des compartiments accessibles en dehors de votre compte AWS. Les compartiments répertoriés sous Compartiments avec accès public sont accessibles par n'importe quel utilisateur d'Internet. Si Access Analyzer for S3 identifie des compartiments publics, vous voyez également un avertissement en haut de la page qui indique le nombre de compartiments publics dans votre région. Les compartiments répertoriés sous Compartiments avec accès à partir d'autres comptes AWS — y compris des comptes AWS tiers sont partagés sous certaines conditions avec d'autres comptes AWS, y compris des comptes extérieurs à votre organisation.

Pour chaque compartiment, Access Analyzer for S3 fournit les informations suivantes :

- Nom du compartiment
- Découvert par Access Analyzer - Lorsque Access Analyzer for S3 a découvert l'accès public ou partagé au compartiment.
- Shared through (Partagé via) - Mode de partage du compartiment via une stratégie de compartiment, une liste de contrôle d'accès (ACL) ou une stratégie de point d'accès. Un compartiment peut être partagé via des stratégies et des listes de contrôle d'accès. Si vous souhaitez rechercher et examiner la source de votre accès au compartiment, vous pouvez utiliser les informations de cette colonne comme point de départ pour prendre des mesures correctives immédiates et précises.
- Statut - Statut du résultat du compartiment. Access Analyzer for S3 affiche les résultats pour tous les compartiments publics et partagés.
  - Actif - Le résultat n'a pas été vérifié.
  - Archivé - Le résultat a été vérifié et confirmé comme prévu.
  - Tous - Tous les résultats pour les compartiments qui sont publics ou partagés avec d'autres comptes AWS, y compris les comptes AWS en dehors de votre organisation.
- Niveau d'accès - Autorisations d'accès accordées pour le compartiment :
  - Liste - Ressources de liste.
  - Lecture - Lire, mais pas écrire les contenus et attributs de ressources.
  - Écriture - Créer, supprimer ou modifier des ressources.
  - Autorisations - Accorder ou modifier des autorisations de ressources.
  - Balisage - Mettre à jour les balises associées à la ressource.

## Activation d'Access Analyzer for S3

Pour utiliser Access Analyzer for S3, vous devez suivre les étapes ci-dessous au préalable.

1. Accordez les autorisations requises.

Pour plus d'informations, consultez [Autorisations requises pour utiliser Access Analyzer](#) dans le IAM Guide de l'utilisateur.

2. Accédez à IAM pour créer un analyseur de niveau compte pour chaque région dans laquelle vous souhaitez utiliser Access Analyzer.

Access Analyzer for S3 nécessite un analyseur au niveau du compte. Pour utiliser Access Analyzer for S3, vous devez créer un analyseur qui utilise un compte comme zone de confiance. Pour plus d'informations, consultez [Activation de Access Analyzer](#) dans IAM Guide de l'utilisateur.

## Blocage de tous les accès publics

Si vous souhaitez bloquer tout accès à un compartiment en un seul clic, vous pouvez utiliser le bouton Block all public access (Bloquer tout accès public) dans Access Analyzer for S3. Lorsque vous bloquez tout accès public à un compartiment, aucun accès public n'est accordé. Nous vous recommandons de bloquer tous les accès publics à vos compartiments, sauf si vous avez besoin d'un accès public pour prendre en charge un cas d'utilisation spécifique et vérifié. Avant de bloquer tout accès public, assurez-vous que vos applications continueront à fonctionner correctement sans accès public.

Si vous ne souhaitez pas bloquer tous les accès publics à votre compartiment, vous pouvez modifier vos paramètres de blocage d'accès public sur la console Amazon S3 pour configurer des niveaux d'accès précis à vos compartiments. Pour plus d'informations, consultez [Utilisation d'Amazon S3 Block Public Access](#) dans le Amazon Simple Storage Service Manuel du développeur.

Dans de rares cas, Access Analyzer for S3 peut ne signaler aucun résultat pour un compartiment qu'une évaluation de blocage d'accès public Amazon S3 signale comme public. Cela se produit parce que le blocage d'accès public Amazon S3 examine les stratégies pour les actions en cours et les actions potentielles qui pourraient être ajoutées à l'avenir, ce qui rend un compartiment public. D'autre part, Access Analyzer for S3 analyse seulement les actions actuelles spécifiées pour le service Amazon S3 dans l'évaluation du statut d'accès.

Pour bloquer tout accès public à un compartiment à l'aide d'Access Analyzer for S3

1. Connectez-vous à 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, sous Dashboards (Tableaux de bord), choisissez Access Analyzer for S3.
3. Dans Access Analyzer for S3, choisissez un compartiment.
4. Choisissez Block all public access (Bloquer tous les accès publics).
5. Pour confirmer votre intention de bloquer tout accès public au compartiment, dans Block all public access (bucket settings) (Bloquer tout accès public (paramètres du compartiment)), entrez **confirm**.

Amazon S3 bloque tout accès public à votre compartiment. Le statut du résultat de compartiment devient resolved (résolu), et le compartiment disparaît de la liste Access Analyzer for S3. Si vous souhaitez vérifier les compartiments résolus, ouvrez IAM Access Analyzer sur la console IAM.

## Vérification et modification de l'accès à un compartiment

Si vous n'aviez pas l'intention d'accorder l'accès aux comptes publics ou à d'autres comptes AWS, y compris les comptes extérieurs à votre entreprise, vous pouvez modifier la liste de contrôle d'accès (ACL) du compartiment, la stratégie du compartiment ou la stratégie de point d'accès pour supprimer l'accès au compartiment. La colonne Shared through (Partagé via) affiche toutes les sources d'accès au compartiment : stratégie de compartiment, ACL de compartiment et/ou stratégie de point d'accès.

Pour consulter et modifier une stratégie de compartiment, une liste ACL de compartiment ou une stratégie de point d'accès

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation, choisissez Access Analyzer for S3.
3. Pour déterminer si l'accès public ou l'accès partagé est accordé via une stratégie de compartiment, une liste de contrôle d'accès de compartiment ou une stratégie de point d'accès, consultez la colonne Shared through (Partagé via).
4. Sous Bucket name (Nom du compartiment), choisissez le nom du compartiment avec la stratégie de compartiment, la liste ACL de compartiment ou la stratégie de point d'accès que vous souhaitez modifier ou vérifier.
5. Si vous souhaitez modifier ou consulter la liste ACL d'un compartiment :
  - a. Choisissez Permissions.
  - b. Choisissez Access Control List.
  - c. Passez en revue la liste ACL de votre compartiment et apportez les modifications nécessaires.

Pour de plus amples informations, veuillez consulter [Comment définir des autorisations de compartiment ACL ? \(p. 127\)](#)

6. Si vous souhaitez modifier ou vérifier une stratégie de compartiment :

- a. Choisissez Permissions.
- b. Choisissez Stratégie de compartiment.
- c. Vérifiez ou modifiez votre stratégie de compartiment selon vos besoins.

Pour de plus amples informations, veuillez consulter [Comment ajouter une stratégie de compartiment S3 ? \(p. 131\)](#)

7. Si vous souhaitez consulter ou modifier une stratégie de point d'accès :

- a. Choisissez Access Points (Points d'accès).
- b. Choisissez le nom du point d'accès.
- c. Vérifiez ou modifiez l'accès en fonction de vos besoins.

Pour plus d'informations, consultez [Gestion et utilisation des points d'accès Amazon S3 \(p. 34\)](#).

Si vous modifiez ou supprimez une liste ACL de compartiment, une stratégie de compartiment ou une stratégie de point d'accès pour supprimer l'accès public ou partagé, le statut du compartiment devient « résolu ». Les résultats de compartiment résolus disparaissent de la liste Access Analyzer for S3, mais vous pouvez les afficher dans IAM Access Analyzer.


## Archivage des résultats de compartiment

Si un compartiment accorde l'accès aux comptes publics ou à d'autres comptes AWS, y compris des comptes extérieurs à votre organisation, pour prendre en charge un cas d'utilisation spécifique (par exemple, un site Web statique, des téléchargements publics ou un partage entre comptes), vous pouvez archiver le résultat du compartiment. Lorsque vous archivez les résultats d'un compartiment, vous confirmez et enregistrez votre intention de le garder public ou partagé. Les résultats des compartiments archivés restent dans votre liste Access Analyzer for S3 afin que vous puissiez toujours savoir quels compartiments sont publics ou partagés.

Pour archiver des résultats de compartiment dans Access Analyzer for S3

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation, choisissez Access Analyzer for S3.
3. Dans Access Analyzer for S3, choisissez un compartiment actif.
4. Pour confirmer votre intention d'autoriser le public ou d'autres comptes AWS (y compris les comptes extérieurs à votre organisation) à accéder à ce compartiment, choisissez Archive (Archiver).
5. Entrez **confirm**, puis choisissez Archive (Archiver).

**Archive findings for bucket with public access** ✕

By archiving the findings for this bucket, you acknowledge that you intend for anyone in the world to be able to access this bucket. If you do not intend for this bucket to be public, use [block public access](#)  to configure secure access to your bucket. Before archiving, review the access granted to this bucket.

To confirm that you intend this bucket to be publicly accessible, enter *confirm* in the box.

Cancel

Confirm

## Activation d'un résultat de compartiment archivé

Après avoir archivé des résultats, vous pouvez toujours les revoir et faire passer leur statut à « actif », ce qui indique que le compartiment nécessite une autre vérification.

Pour activer un résultat de compartiment archivé dans Access Analyzer for S3

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation, choisissez Access Analyzer for S3.
3. Choisissez les résultats de compartiment archivés.
4. Choisissez Mark as active (Marquer comme actif).

## Affichage des détails de résultats

Si vous avez besoin de plus d'informations sur un compartiment, vous pouvez ouvrir les détails de résultat du compartiment dans IAM Access Analyzer, dans la console IAM.

Pour afficher les détails de résultats dans Access Analyzer for S3

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation, choisissez Access Analyzer for S3.
3. Dans Access Analyzer for S3, choisissez un compartiment.
4. Choisissez Afficher les détails.

Les détails de résultats s'ouvrent dans IAM Access Analyzer, dans la console IAM.

## Téléchargement d'un rapport Access Analyzer for S3

Vous pouvez télécharger vos résultats de compartiment sous la forme d'un rapport CSV que vous pouvez utiliser à des fins d'audit. Le rapport contient les mêmes informations que celles que vous voyez dans Access Analyzer for S3 sur la console Amazon S3.

Pour télécharger un rapport

1. Ouvrez la console Amazon S3 à l'adresse <https://console.aws.amazon.com/s3/>.
2. Dans le volet de navigation de gauche, choisissez Access Analyzer for S3.
3. Dans le filtre de région, sélectionnez la région.

Access Analyzer for S3 effectue une mise à jour afin d'afficher les compartiments pour la région sélectionnée.

4. Choisissez Download report (Télécharger le rapport).

Un rapport CSV est généré et enregistré sur votre ordinateur.



# Historique du document

Dernière mise à jour de la documentation : 27 mars 2019

Le tableau ci-après décrit les modifications importantes dans chaque édition du Amazon Simple Storage Service Guide de l'utilisateur de la console à partir du 19 juin 2018. Pour recevoir les notifications des mises à jour de cette documentation, abonnez-vous à un flux RSS.

update-history-change	update-history-description	update-history-date
<a href="#">Nouvelle classe de stockage d'archive</a> (p. 140)	Amazon S3 propose désormais une nouvelle classe de stockage d'archive, S3 Glacier Deep Archive, pour le stockage d'objets rarement consultés. Pour plus d'informations, consultez <a href="#">Comment restaurer un objet S3 qui a été archivé ?</a> et <a href="#">Classes de stockage</a> dans le Amazon Simple Storage Service Manuel du développeur.	March 27, 2019
<a href="#">Blocage d'accès public des compartiments S3</a> (p. 140)	Le blocage de l'accès public Amazon S3 empêche l'application de paramètres qui autorisent un accès public aux données dans des compartiments S3. Pour plus d'informations, consultez <a href="#">Blocage d'accès public des compartiments S3</a> .	November 15, 2018
<a href="#">Filtrage des améliorations dans les règles de la réplication entre régions (CRR)</a> (p. 140)	Dans une règle CRR, vous pouvez spécifier un filtre d'objet pour choisir un sous-ensemble des objets auquel s'applique la règle. Précédemment, vous ne pouviez filtrer que sur un préfixe de clé d'objet. Dans cette version, vous pouvez filtrer sur un préfixe de clé d'objet, une ou plusieurs balises d'objet, ou les deux. Pour de plus amples informations, veuillez consulter <a href="#">Comment ajouter une règle de réplication à un compartiment S3 ?</a> .	September 19, 2018
<a href="#">Mises à jour disponibles sur RSS</a> (p. 140)	Vous pouvez à présent vous abonner à un flux RSS pour recevoir les notifications des mises à jour du Amazon Simple	June 19, 2018

Storage Service Guide de  
l'utilisateur de la console.

## Mises à jour antérieures

Le tableau ci-après décrit les modifications importantes dans chaque édition du Amazon Simple Storage Service Guide de l'utilisateur de la console publiée avant le 19 juin 2018.

Modification	Description	Date de modification
Nouvelle classe de stockage	Amazon S3 propose désormais une nouvelle classe de stockage, ONEZONE_IA (où « IA » signifie « infrequent access », ou accès peu fréquent) pour le stockage d'objets. Pour de plus amples informations, veuillez consulter <a href="#">Classes de stockage</a> dans le manuel Amazon Simple Storage Service Manuel du développeur.	4 avril 2018
Prise en charge des fichiers d'inventaire Amazon S3 au format ORC	Amazon S3 prend désormais en charge le format <a href="#">Apache ORC (Optimized Row Columnar)</a> en plus du format de fichier CSV (à valeurs séparées par une virgule) pour les fichiers de sortie d'inventaire. Pour plus d'informations, consultez <a href="#">Comment configurer l'inventaire Amazon S3 ? (p. 109)</a> .	17 novembre 2017
Vérification des autorisations de compartiment	La vérification des autorisations de compartiment dans la console Amazon S3 vérifie les stratégies de compartiment et les listes de contrôle d'accès (ACL) de compartiment pour identifier les compartiments accessibles publiquement. La vérification des autorisations de compartiment facilite l'identification des compartiments S3 qui fournissent un accès public en lecture et en écriture.	06 novembre 2017
Chiffrement par défaut pour les compartiments S3	Le chiffrement par défaut d'Amazon S3 fournit un moyen de définir le comportement de chiffrement par défaut pour un compartiment S3. Vous pouvez définir le chiffrement par défaut sur un compartiment afin que tous les objets soient chiffrés lorsqu'ils sont stockés dans le compartiment. Les objets sont chiffrés au moyen du chiffrement côté serveur avec des clés gérées par Amazon S3 (SSE-S3) ou par AWS KMS (SSE-KMS). Pour plus d'informations, consultez <a href="#">Comment activer le chiffrement par défaut pour un compartiment Amazon S3 ? (p. 9)</a> .	06 novembre 2017
État du chiffrement dans l'inventaire Amazon S3	Amazon S3 prend désormais en charge l'inclusion de l'état de chiffrement dans l'inventaire Amazon S3 afin que vous puissiez voir comment vos objets sont chiffrés au repos pour des audits de conformité ou à d'autres fins. Vous pouvez également configurer le chiffrement de l'inventaire Amazon S3 avec le chiffrement côté serveur (SSE) ou SSE-KMS afin que tous les fichiers d'inventaire soient chiffrés en conséquence. Pour plus d'informations, consultez <a href="#">Comment configurer l'inventaire Amazon S3 ? (p. 109)</a> .	06 novembre 2017
Améliorations de la réplication entre régions	La réplication entre régions prend désormais en charge les aspects suivants : <ul style="list-style-type: none"><li>Par défaut, Amazon S3 ne réplique pas les objets de votre compartiment source qui sont créés à l'aide du chiffrement côté</li></ul>	06 novembre 2017

Modification	Description	Date de modification
	<p>serveur au moyen de clés gérées par AWS KMS. Vous pouvez désormais configurer une règle de réplication pour répliquer ces objets. Pour de plus amples informations, veuillez consulter <a href="#">Comment ajouter une règle de réplication à un compartiment S3 ? (p. 87)</a>.</p> <ul style="list-style-type: none"><li>• Dans un scénario à plusieurs comptes, vous pouvez configurer une règle de réplication pour remplacer le propriétaire des réplicas par le compte AWS qui détient le compartiment de destination. Pour de plus amples informations, veuillez consulter <a href="#">Ajout d'une règle de réplication lorsque le compartiment de destination est dans un compte AWS distinct (p. 96)</a>.</li></ul>	
Documentation et fonctionnalités supplémentaires	La console Amazon S3 prend désormais en charge l'activation de la journalisation au niveau des objets pour un compartiment S3 avec la journalisation des événements de données AWS CloudTrail. Pour plus d'informations, consultez <a href="#">Comment activer la journalisation au niveau des objets pour un compartiment S3 avec des événements de données AWS CloudTrail ? (p. 15)</a> .	19 octobre 2017
L'ancienne console Amazon S3 n'est plus disponible	L'ancienne version de la console Amazon S3 n'est plus disponible et l'ancien manuel d'utilisation a été retiré du site de documentation Amazon S3.	31 août 2017
Disponibilité générale de la nouvelle console Amazon S3	La disponibilité générale de la nouvelle console Amazon S3 est annoncée.	15 mai 2017

# Glossaire AWS

Pour la terminologie AWS la plus récente, consultez le [Glossaire AWS](#) dans le document AWS General Reference.